ProLegis

REC-RDAT-TRAI-AG-2016

Action grants to support training activities on the data protection reform

REC PROGRAMME

GA No. 769143

Preparing local public authorities for the new data Protection Legislation

ProLegis

WP2: Training Support

D2.2 Training Materials

Lead partner: LIF

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

Project co-funded by the European Commission within the Rights, Equality and Citizenship Programme (2014-2020)		
Dissemination Level:		
PU	Public	X
CO	Confidential, only for members of the consortium (including the Commission Services)	
EU-RES	Classified Information: RESTREINT UE (Commission Decision 2005/444/EC)	
EU-CON	Classified Information: CONFIDENTIEL UE (Commission Decision 2005/444/EC)	
EU-SEC	Classified Information: SECRET UE (Commission Decision 2005/444/EC)	
Document version control:		
Version 1	Developed by: Martin Zahariev, LIF	17.04.2018
Version 1	Revised by: Daniela Ilieva-Koleva, LIF	23.04.2018
Version 2	Updated by: Christof Tschohl, VICESSE	29.05.2018
Version 2	Updated by: Denitsa Kozhuharova, LIF	26.07.2018

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

ProLegis

Legal Grounds for Personal Data Processing

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

ProLegis

Contents

1. LEGAL FRAMEWORK 4
   1.1. Charter of Fundamental Rights of EU 4
   1.2. GDPR 4
2. LEGAL GROUNDS FOR PERSONAL DATA PROCESSING UNDER GDPR 10
   2.1. Consent 10
      2.1.1. Meaning & legal requirements 10
      2.1.2. Applicability in the context of the Local authorities' activity 12
   2.2. Performance/ conclusion of contract with the data subject 13
      2.2.1. Meaning & legal requirements 13
      2.2.2. Applicability in the context of the Local authorities' activity 14
   2.3. Legal obligation 15
      2.3.1. Meaning & legal requirements 15
      2.3.2. Applicability in the context of the Local authorities' activity 16
   2.4. Vital interest 16
      2.4.1. Meaning & legal requirements 16
      2.4.2. Applicability in the context of the Local authorities' activity 17
   2.5. Task carried out in the public interest/ exercise of official authority 17
      2.5.1. Meaning & legal requirements 17
      2.5.2. Applicability in the context of the Local authorities' activity 18
   2.6. Legitimate Interests 18
      2.6.1. Meaning & legal requirements 18
      2.6.2. Applicability in the context of the Local authorities' activity 19
3. CONCLUSION & PRACTICAL ADVICES 19

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

4. EXTERNAL SOURCES & WEBLINKS 20
Books 20
Documents of the Article 29 Working Party 20
Web Links 20
5. REFERENCES 21

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

1. LEGAL FRAMEWORK

1.1. Charter of Fundamental Rights of EU

Article 8

Protection of personal data

1. Everyone has the right to the protection of personal data concerning him or her.

*2. Such data must be processed fairly for specified purposes and **on the basis of the consent of the person concerned or some other legitimate basis laid down by law**. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.*

3. Compliance with these rules shall be subject to control by an independent authority.

1.2. GDPR

Recital (42)

[…] For consent to be informed, the data subject should be aware at least of the identity of the controller and the purposes of the processing for which the personal data are intended. Consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment.

Recital (43)

*In order to ensure that consent is freely given, consent should not provide a valid legal ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject and the controller, **in particular where the controller is a public authority** and it is therefore unlikely that consent was freely given in all the circumstances of that specific situation. Consent is presumed not to be freely given if it does not allow separate consent to be given to different personal data processing operations despite it being appropriate in the individual case, or if the performance of a contract, including the provision of a service, is dependent on the consent despite such consent not being necessary for such performance.*

Recital (44)

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

Processing should be lawful where it is ***necessary in the context of a contract or the intention to enter into a contract.***

Recital (45)

Where processing is carried out in accordance with a ***legal obligation*** *to which the controller is subject or where processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority, the processing should have a basis in Union or Member State law. This Regulation does not require a specific law for each individual processing. A law as a basis for several processing operations based on a legal obligation to which the controller is subject or where processing is necessary for the performance of a task carried out in the public interest or in the exercise of an official authority may be sufficient. It should also be for Union or Member State law to determine the purpose of processing. Furthermore, that law could specify the general conditions of this Regulation governing the lawfulness of personal data processing, establish specifications for determining the controller, the type of personal data which are subject to the processing, the data subjects concerned, the entities to which the personal data may be disclosed, the purpose limitations, the storage period and other measures to ensure lawful and fair processing. It should also be for Union or Member State law to determine whether the controller performing a task carried out in the public interest or in the exercise of official authority should be a public authority or another natural or legal person governed by public law, or, where it is in the public interest to do so, including for health purposes such as public health and social protection and the management of health care services, by private law, such as a professional association.*

Recital (46)

The processing of personal data should also be regarded to be lawful where it is necessary to protect an ***interest which is essential for the life of the data subject or that of another natural person****. Processing of personal data based on the vital interest of another natural person should in principle take place only where the processing cannot be manifestly based on another legal basis. Some types of processing may serve both important grounds of public interest and the vital interests of the data subject as for instance when processing is necessary for humanitarian purposes, including for monitoring epidemics and their spread*

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

or in situations of humanitarian emergencies, in particular in situations of natural and man-made disasters.

Recital (47)

*The **legitimate interests of a controller, including those of a controller to which the personal data may be disclosed, or of a third party**, may provide a legal basis for processing, provided that the interests or the fundamental rights and freedoms of the data subject are not overriding, taking into consideration the reasonable expectations of data subjects based on their relationship with the controller. Such legitimate interest could exist for example where there is a relevant and appropriate relationship between the data subject and the controller in situations such as where the data subject is a client or in the service of the controller. At any rate the existence of a legitimate interest would need careful assessment including whether a data subject can reasonably expect at the time and in the context of the collection of the personal data that processing for that purpose may take place. The interests and fundamental rights of the data subject could in particular override the interest of the data controller where personal data are processed in circumstances where data subjects do not reasonably expect further processing. Given that it is for the legislator to provide by law for the legal basis for public authorities to process personal data, that legal basis should not apply to the processing by public authorities in the performance of their tasks. The processing of personal data strictly necessary for the purposes of preventing fraud also constitutes a legitimate interest of the data controller concerned. The processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest.*

Recital (48)

Controllers that are part of a group of undertakings or institutions affiliated to a central body may have a legitimate interest in transmitting personal data within the group of undertakings for internal administrative purposes, including the processing of clients' or employees' personal data. The general principles for the transfer of personal data, within a group of undertakings, to an undertaking located in a third country remain unaffected.

Recital (49)

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

The processing of personal data to the extent strictly necessary and proportionate for the purposes of ensuring network and information security, i.e. the ability of a network or an information system to resist, at a given level of confidence, accidental events or unlawful or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted personal data, and the security of the related services offered by, or accessible via, those networks and systems, by public authorities, by computer emergency response teams (CERTs), computer security incident response teams (CSIRTs), by providers of electronic communications networks and services and by providers of security technologies and services, constitutes a legitimate interest of the data controller concerned. This could, for example, include preventing unauthorised access to electronic communications networks and malicious code distribution and stopping 'denial of service' attacks and damage to computer and electronic communication systems.

Recital (50)

The processing of personal data for purposes other than those for which the personal data were initially collected should be allowed only where the processing is compatible with the purposes for which the personal data were initially collected. In such a case, no legal basis separate from that which allowed the collection of the personal data is required. If the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, Union or Member State law may determine and specify the tasks and purposes for which the further processing should be regarded as compatible and lawful. Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes should be considered to be compatible lawful processing operations. The legal basis provided by Union or Member State law for the processing of personal data may also provide a legal basis for further processing. In order to ascertain whether a purpose of further processing is compatible with the purpose for which the personal data are initially collected, the controller, after having met all the requirements for the lawfulness of the original processing, should take into account, inter alia: any link between those purposes and the purposes of the intended further processing; the context in which the personal data have been collected, in particular the reasonable expectations of data subjects based on their relationship with the controller as to their further use; the nature of the personal data; the consequences of the intended further processing for data subjects; and the existence of appropriate safeguards in both the original and intended further processing operations.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

Where the data subject has given consent or the processing is based on Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard, in particular, important objectives of general public interest, the controller should be allowed to further process the personal data irrespective of the compatibility of the purposes. In any case, the application of the principles set out in this Regulation and in particular the information of the data subject on those other purposes and on his or her rights including the right to object, should be ensured. Indicating possible criminal acts or threats to public security by the controller and transmitting the relevant personal data in individual cases or in several cases relating to the same criminal act or threats to public security to a competent authority should be regarded as being in the legitimate interest pursued by the controller. However, such transmission in the legitimate interest of the controller or further processing of personal data should be prohibited if the processing is not compatible with a legal, professional or other binding obligation of secrecy.

Article 4

Definitions

For the purposes of this Regulation:

[…]

(11) 'consent' of the data subject means any ***freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or he****r;*

Article 6

Lawfulness of processing

1. *Processing shall be lawful only if and to the extent that* ***at least one of the following applies:***

(a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

(c) processing is necessary for compliance with a legal obligation to which the controller is subject;

(d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;

(e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks.

2. Member States may maintain or introduce more specific provisions to adapt the application of the rules of this Regulation with regard to processing for compliance with points (c) and (e) of paragraph 1 by determining more precisely specific requirements for the processing and other measures to ensure lawful and fair processing including for other specific processing situations as provided for in Chapter IX.

3. The basis for the processing referred to in point (c) and (e) of paragraph 1 shall be laid down by:

(a) Union law; or

(b) Member State law to which the controller is subject.

The purpose of the processing shall be determined in that legal basis or, as regards the processing referred to in point (e) of paragraph 1, shall be necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. That legal basis may contain specific provisions to adapt the application of rules of this Regulation, inter alia: the general conditions governing the lawfulness of processing by the controller; the types of data which are subject to the processing; the data subjects concerned; the entities to, and the

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

purposes for which, the personal data may be disclosed; the purpose limitation; storage periods; and processing operations and processing procedures, including measures to ensure lawful and fair processing such as those for other specific processing situations as provided for in Chapter IX. The Union or the Member State law shall meet an objective of public interest and be proportionate to the legitimate aim pursued.

4. Where the processing for a purpose other than that for which the personal data have been collected is not based on the data subject's consent or on a Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 23(1), the controller shall, in order to ascertain whether processing for another purpose is compatible with the purpose for which the personal data are initially collected, take into account, inter alia:

(a) any link between the purposes for which the personal data have been collected and the purposes of the intended further processing;

(b) the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller;

(c) the nature of the personal data, in particular whether special categories of personal data are processed, pursuant to Article 9, or whether personal data related to criminal convictions and offences are processed, pursuant to Article 10;

(d) the possible consequences of the intended further processing for data subjects;

(e) the existence of appropriate safeguards, which may include encryption or pseudonymisation.

2. LEGAL GROUNDS FOR PERSONAL DATA PROCESSING UNDER GDPR

2.1. Consent

2.1.1. Meaning & legal requirements

Consent is one of the six legal grounds listed in Art. 6 of the GDPR. In order to be valid, GDPR requires the consent to be freely given, specific, informed and unambiguous.

- **'free'** = implies real choice and control for data subjects[i]. If any unfavorable consequences occur for the data subject in case they do not consent for the processing/ withdraws already given consent (e.g. denial of service, higher costs

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

for goods/ service – fees, price, etc.), the consent should be considered not freely given. Due to the imbalance of powers between public authorities and data subjects, consent would rarely be useful tool for data processing in the context of exercising official authorities;

- **'specific'** = tightly connected with the requirement that the data subject consents for one or more specific purposes of the processing (so called 'granularity' of the consent[ii]) and the purpose specification principle. Each of the purposes for data processing needs to be clearly defined from the outset for the data subject. The data subject should be able to choose for which purposes to consent (e.g. to consent for purpose A, B and C and not to consent for purpose E and D). The information related to consent should be clearly separated from information related to any other matters. A consent must be obtained for any new processing purpose and the controllers should provide specific information with each separate consent request about the data that are processed for each purpose;
- **'informed'** = the minimum requirements under GDPR include provision of information for the data controller and the purposes of the processing. Article 29 Working Party (WP29) recommends the inclusion of additional information such as the type of data collected and used; the right to withdraw consent; information about the use of the data for decisions based solely on automated processing, including profiling[iii]; in case of transfers – information about the possible risks of data transfers to third countries in the absence of an adequacy decision and appropriate safeguards[iv].
- **'unambiguous'** = consent must be given via a statement from the data subject or a clear affirmative act. Consent must always be given through an active motion or declaration. Thus, silence, pre-ticked boxes and inactivity cannot constitute valid consent under GDPR;
- **As easily withdrawn as given** = consent could be withdrawn at any time. This should not necessarily happen under with the same action, but the process of withdrawing should be as easy as the process of giving consent (e.g. clicking a box in online declaration for consenting to receive the municipality newspaper is as easy as clicking a link in the body of the email accompanying the newsletter for unsubscribing and withdrawing the consent);
- **Specific requirements regarding consent from children** = GDPR treats children as a vulnerable category of data subjects. Thus, they merit special protection, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data. In case of provision of information society services offered to a child (e.g. online educational

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

campaigns conducted on municipalities' website which require collection of children personal data), consent for the processing of children's data under 16 years of age (the member states may lower this age to 13 years) should be obtained from or authorized by the holder of parental responsibility over the child;

- **Consent under Directive 95/46** = consent already obtained under the old regime should not necessarily need to be revised. If the consent corresponds to the requirements set in GDPR, then the consent obtained under the Directive should continue to be valid ground for the processing.

The data controller has the burden of proof to demonstrate that consent has been duly obtained[v].

2.1.2. Applicability in the context of the Local authorities' activity

In practice, consent will rarely be the basic legal ground on which the Local authorities (LAs) will legitimately process personal data of citizens. This conclusion derives out of the GDPR requirements which consent must meet in order to be valid.

First, the fact that consent should be 'freely given', i.e. no adverse consequences should be caused to the data subject in case no consent is given, means that in any situation in which specific LA acts as a holder of public power, consent could not be used as a valid legal ground for processing. The control for the duly performance of citizens' public obligations (e.g. collecting of local fees and taxes, registration of acquisition of real estates/ vehicles, etc.) and the imposition of sanctions in case of non-performance of such obligations are inherently connected with the right (and obligation) to exercise coercive powers. This means that the data subjects have not real free choice to consent or not to consent for the processing of their personal data. They are in subordinate position and are obliged by law to cooperate to LA.

Second, consent could be withdrawn 'at any time'. If consent was the legitimate ground for processing of personal data in case citizens perform their legal obligations, potentially any citizen acting in bad faith (e.g. not-willing to perform certain public obligation) could withdraw their consent at any time and could use this withdrawal to create obstacles (and in practice 'to block') the normal functioning of LA. If the consent is withdrawn, LA as data controller should terminate the processing. This is unthinkable when exercising official authorities, because it will jeopardize the entire idea of exercising public power.

Thus, in the situations described above consent is not the right tool for such processing.

According to WP29, *'the use of consent as a lawful basis for data processing by public authorities* ***is not totally excluded*** *under the legal framework of the GDPR'*[vi]. Thus, consent

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

might be useful tool in situations in which LA either does not exercise its typical and main functions or the respective processing is rather optional (and there are default processing procedures established that shall take place in case the data subject does not consent). Examples are the following situations:

- LA and government authorities require the same information for issuing certain legal act upon request of a citizen but are unable to access each other's databases. As they both ask for the same information from the citizen, they could ask for the citizen's consent to merge the files, to avoid duplicate procedures and correspondence. Both public bodies should ensure that this is optional and that issuance of the document would be ensured even if the citizen does not consent to the merger of the data[vii];
- LA provides for the option to notify citizens participating in administrative proceedings before them via e-mail. The regime is opt-in, i.e. the citizens are free to decide whether to be notified via e-mail (e.g. by ticking box in online/ paper form available and providing their email). In case of refusal to consent/ withdrawal of the consent, LA should have a default procedure for notification (e.g. by registered mail). The processing of the email in such a case would be based on consent;
- LA provides to the citizens the option to subscribe for receiving invitations for various activities organized by LA (e.g. exhibitions in local museums, theatre premiers in the municipality theatre, garbage collection campaigns, competitions/ educational campaigns conducted in the municipality schools). The subscription requires provision of contact data (e.g. post address, phone number, e-mail, etc.) as well as data for the preferences of the data subjects (e.g. hobbies, interests, etc.). The processing of such data would be based on consent, as the citizens are entitled to unsubscribe from such notifications freely at any time without detriment.

2.2. Performance/ conclusion of contract with the data subject

2.2.1. Meaning & legal requirements

The provision of Art. 6, Para 1, item "b" of GDPR introduces two **separate** legal grounds for personal data processing:

(i) situations where the processing is necessary for the performance of the contract to which the data subject is a party;

(ii) situations where the processing that takes place *prior to* entering into a contract. This covers pre-contractual relations, provided that steps are taken at the request of the data subject, rather than at the initiative of the controller or any third party[viii].

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

The first hypothesis should be interpreted strictly and should not cover situations where the processing is not genuinely necessary for the performance of a contract, but rather unilaterally imposed on the data subject by the controller[ix]. According to the interpretation given by WP29 for the same ground under the old Directive 95/ 46, the said legal ground only applies to what is necessary for the performance of a contract. In other words, as long as processing covers the normal execution of a contract, it could fall within the said legal ground. This legal ground would cover situations when the processing takes place in the context of a contract irrespective of which phase of the contract is concerned[x]. However, any further actions triggered by non-compliance or to all other incidents in the execution of a contract do not fall within the scope of this legal ground. Such types of processing would require the application of different legal ground – e.g. overriding legitimate interest of the data controller.

The second hypothesis could include processing necessary for preparation of offers, recruitment for HR activities, etc. However, any detailed background checks of the candidates would be rather extensive and would not be justified as steps requested by the data subject.

In general, this legal ground is interpreted narrowly by regulators, so the controllers should be able to demonstrate that the processing is unavoidable in order to complete the contract[xi].

2.2.2. Applicability in the context of the Local authorities' activity

This legal ground for processing of personal data could be applied by the LAs at least in the following areas:

- Processing in the employment context – e.g. processing salary information and bank account details so that salaries could be paid[xii];
- Processing in the context of conclusion of contracts for public procurements – this contractual legal ground could overlap with another legal ground for personal data processing – e.g. LA's legal obligation for personal data processing within the respective administrative procedure imposed by the local law;
- Processing in the context of the relationships between some private entities wholly/ partially owned by the municipality/ state and the citizens – e.g. entities providing public transport services within the entire city/ village, entities providing utility services (electricity-, gas-, water supply, etc.) when concluding the respective contracts.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

2.3. Legal obligation

2.3.1. Meaning & legal requirements

This legal ground requires a clear legal provision introduced either on legislative or on sublegislative (the so called in some Member States secondary legislation) level that obliges the controller to conduct the processing. WP29 highlights that the law must fulfil all relevant conditions to make the obligation valid and binding, and must also comply with data protection law, including the requirement of necessity, proportionality and purpose limitation[xiii]. GDPR explicitly requires that this obligation must cumulatively be:

(i) an obligation of Member State or EU law to which the controller is subject. WP29 has already made the following interpretation under the old Directive 95/46 in that respect: obligations under the laws of third countries (such as, for example, the obligation to set up whistleblowing schemes under the Sarbanes–Oxley Act of 2002 in the United States) are not covered by the ground legal obligation. In order to be valid, a legal obligation of a third country would need to be officially recognized and integrated in the legal order of the Member State concerned, e.g. under the form of an international agreement; and

(ii) 'clear and precise' and its application foreseeable for those subject to it. The recitals 41 and 45 of GDPR make it clear that the relevant 'legal obligation' need not be statutory which could have practical implications for common law countries – it would be sufficient, if this meets the 'clear and precise' test. A legal obligation could cover several processing operations carried out by the controller so that it may not be necessary to identify a specific legal obligation for each individual processing activity[xiv].

WP29 has indicated that in order to apply this legal ground, the controller must not have a choice whether or not to fulfil the obligation. Voluntary unilateral engagements and public-private partnerships processing data beyond what is required by law are thus not covered by this legal ground[xv]. The legal obligation as a ground for personal data processing should apply on the basis of legal provisions referring explicitly to the nature and object of the processing. The controller should not have an undue degree of discretion on how to comply with the legal obligation[xvi].

WP29 explicitly acknowledges that the legislation may in some cases set only a general objective, while more specific obligations are imposed at a different level (e.g. in secondary legislation or by a binding decision of a public authority). According to WP29, this may also lead to legal obligations provided that the nature and object of the processing is well defined and subject to an adequate legal basis[xvii].

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

2.3.2. Applicability in the context of the Local authorities' activity

In practice, this legal ground would be one of the most important legal grounds for personal data processing conducted by LAs. This legal ground would cover both situations related to providing administrative services/ facilitating the performance of public obligations of the citizens and fulfilling certain specific obligations of the LAs in their capacity of employers. This legal ground could apply e.g. in the following situations:

- collection of data by LA for the handling of penalties for parking at unauthorized locations;
- reporting of salary data of the LA's employees to social security or tax authorities[xviii].

2.4. Vital interest

2.4.1. Meaning & legal requirements

This legal ground is to be interpreted very narrowly. WP29 has also acknowledged that the vital interest should have a limited application[xix]. The notion of 'vital interest' is inherently connected with imminent threat for fundamental goods of the data subject (life, health, body integrity, etc.). In the legal doctrine it is indicated that the processing contemplated should be vital to an individual's survival[xx]. According to WP29's interpretation under the old Directive 95/46, the threat should be **immediate**, i.e. collecting and processing personal data on a large scale for purely preventive purposes could not fall within the scope of this legal ground[xxi]. Recital 46 of GDPR explicitly authorizes processing on this legal ground for humanitarian purposes, including for monitoring epidemics and their spread or in situations of humanitarian emergencies, in particular in situations of natural and man-made disasters (in these scenarios there might be overlapping with both the important grounds of public interest and the vital interest). Thus, this strict interpretation imposed by WP29 might be 'softened' in future.

It should also be noted that under the old Directive 95/46 the legal ground 'vital interest' related only to the interest of the data subject. With GDPR the scope of this legal ground has a broader scope – the vital interest could be either of the data subject or of another natural person. GDPR explicitly requires that processing of personal data based on the vital interest of another natural person should in principle take place only where the processing cannot be **manifestly** based on another legal basis. In other words, basing the processing on the vital interest would be rather a 'last resort' solution for the controllers.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

2.4.2. Applicability in the context of the Local authorities' activity

The possibility to apply this ground in the context of LA activities is rather limited. This legal ground could theoretically be applied in a very limited number of cases, e.g. to justify process personal data of employees or citizens in case of emergency situations occurred within the jurisdiction of the LA and if there is no other legal ground for such processing (e.g. legal obligation or exercising official authority).

2.5. Task carried out in the public interest/ exercise of official authority

2.5.1. Meaning & legal requirements

The task or the authority of the data controller should be laid down in the EU law or in the Member State law to which the controller is subject. Tasks carried out in the public interest of a third country or in the exercise of an official authority granted under foreign law do not fall within the scope of this provision under the old Directive 95/46[xxii] and this approach is continued with GDPR.

The analogue of this provision under the old Directive used to cover two different situations:

(i) where the controller itself has an official authority or a public interest task (but not necessarily is obliged to process data) and the processing is necessary for exercising that authority or performing that task, or

(ii) where the controller does not have an official authority but is requested by a third party having such authority to disclose data[xxiii].

GDPR has removed the second criterion, i.e. situations where the exercise of official authority is vested in a party to whom the data are disclosed is no longer relevant as a ground for data processing[xxiv]. In other words, the circumstances in which a controller can rely on this legal ground are narrower than before.

The official authority or public task should typically be attributed in statutory laws or other legal regulations. WP29 has explicitly acknowledged that after GDPR this legal ground need to be interpreted in a way as to allow public authorities some degree of flexibility for ensuring their proper management and functioning. Thus, such activities should fall outside the scope of this legal ground and could processing of personal data could be based on the legitimate interest ground[xxv].

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

Last but not least, it should be noted that the data subjects are entitled to object against processing based on this legal ground. It is the controller who has the burden to demonstrate that it has compelling legitimate grounds to process the personal data[xxvi].

2.5.2. Applicability in the context of the Local authorities' activity

Among with the legal obligation under Art. 6, Para 1, item 'c' of GDPR, the task carried out in the public interest/ exercise of official authority would be one of the most important legal grounds for the LAs' activities. Examples made by WP29 for the application of this ground include:

- a tax authority that collects and processes an individual's tax return in order to establish and verify the amount of tax to be paid – by analogy this ground could be applied also for LAs which administer local taxes;
- a local government body (e.g. a municipal authority) entrusted with the task of running a library service, a school, or a local swimming pool.

2.6. Legitimate Interests

2.6.1. Meaning & legal requirements

The legal ground 'legitimate interests' includes two elements:

(i) Legitimate interest of the data controller/ third parties:
   a. The concept of 'interest' is defined by WP29 as a broader stake that a controller may have in the processing, or the benefit that the controller derives – or that society might derive – from the processing[xxvii]. The interest might benefit to the society in general but might also be beneficial only for the respective data controller/ third party;
   b. The concept of 'legitimacy' is inherently connected with the compliance with the law – both data protection law and the laws applicable to the respective activity of the controller. In other words, any illegal goals pursued by the controller/ the third party would disqualify the applicability of this legal ground. WP29 has made a non-exhaustive listing of the most common scenarios in which the legitimate interest under the old Directive 95/46 could be applied. The areas vary from advertising/ attention-gaining purposes (e.g. direct marketing, advertising or unsolicited non-commercial messages, including for political campaigns or charitable fundraising) to society-beneficial activities (e.g. whistle-blowing schemes, exercising the right to

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

freedom of expression or information or prevention of fraud, misuse of services, or money laundering).

(ii) The legitimate interest should override the interests, fundamental rights and freedoms and the data subject = a balancing test should be applied on a case by case basis. This requirement is inherently connected with the proportionality principle. Although the data controller/ third party may have legitimate interest to conduct the processing, this might be disproportionate (e.g. the respective processing might be too intrusive, on too large scale, without proper limitations and safeguards, etc.) and in such a scenario the processing would not be justified as lawful. WP29 has stated that among the factors necessary to make the balancing test are:

a. assessing the controller's legitimate interest;
b. impact on the data subjects;
c. provisional balance and
d. additional safeguards applied by the controller to prevent any undue impact on the data subjects[xxviii].

2.6.2. Applicability in the context of the Local authorities' activity

GDPR significantly limits the applicability of the legitimate interest ground in the context of the public authorities' activities. GDPR explicitly provides that this legal ground shall not apply to processing carried out by public authorities in the performance of their tasks. The rationale behind this provision is that that public authorities should be authorized by law to perform their tasks.

Thus, it is advisable for LAs that rely on legitimate interest for performing their tasks to reconsider which other legal ground for personal data processing they could apply (e.g. task in public interest/ official authority).

However, the legitimate interest could still be applied by LAs as a valid legal ground for their internal processes – e.g. in their HR activities.

3. CONCLUSION & PRACTICAL ADVICES

The ability to determine which legal ground is applicable for which processing activity is essential for each data controller in order to ensure the lawfulness of the processing. Moreover, the information which legal ground applies to which purpose of processing is one of the key elements of the transparency principle, as it is explicitly included among the information that must be provided to each data subject by the controller (Art. 13 and Art. 14 of GDPR).

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

Therefore, both public and private data controllers should be well aware of the meaning of each of the legal grounds listed in Art. 6 of GDPR. The Regulation does not provide for new legal grounds, but rather amends the requirements and the conditions for applicability for some of the existing ones (e.g. consent, legitimate interests). In any case, being able to identify the correct legal ground is the first step towards ensuring GDPR compliance within the organization. In the doctrine it is indicated that a prudent data controller should take the necessary steps in order to guarantee that in cases where the supervisory authorities require evidence, the controller should be able to point to which criteria it relies for the processing and its proper notification to the data subjects[xxix].

4. EXTERNAL SOURCES & WEBLINKS

Books

- **Voigt, P., von dem Bussche, A.**, The EU General Data Protection Regulation (GDPR) – A Practical Guide, Springer International Publishing (2017);
- **Boardman, R., Mullock, J., Mole, A.** Bird & Bird Guide to General Data Protection Regulation (2016);
- **EU** General Data Protection Regulation (GDPR). An Implementation and Compliance Guide, IT Governance Publishing, Cambridgeshire (2016);
- **European** Data Protection. Law and Practice, Executive Editor: Edurado Ustaran, CIPP/E, Partner, Hogan Lovells, IAPP (2018);

Documents of the Article 29 Working Party

- WP29, Guidelines on Consent under Regulation 2016/679, WP 259;
- WP29, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, WP 217;

Web Links

- http://europa.eu/rapid/press-release_IP-18-386_en.htm
- https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en
- https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/grounds-processing/when-can-personal-data-be-processed_en

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

- https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/grounds-processing/what-does-grounds-legitimate-interest-mean_en
- https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/grounds-processing/when-consent-valid_en
- https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/grounds-processing/does-consent-given-25-may-2018-continue-be-valid-once-gdpr-starts-apply-25-may-2018_en
- https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/grounds-processing/what-if-somebody-withdraws-their-consent_en
- https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/grounds-processing/what-if-somebody-withdraws-their-consent_en

5. REFERENCES

[i] WP29, Guidelines on Consent under Regulation 2016/679, WP 259, p. 6.
[ii] WP29, Guidelines on Consent under Regulation 2016/679, WP 259, p. 11-12.
[iii] More information on profiling is available in WP29 Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (project).
[iv] WP29, Guidelines on Consent under Regulation 2016/679, WP 259, p. 13.
[v] EU General Data Protection Regulation (GDPR). An Implementation and Compliance Guide, IT Governance Publishing, Cambridgeshire (2016), p. 189-190.
[vi] WP29, Guidelines on Consent under Regulation 2016/679, WP 259, p. 7.
[vii] The example is given in WP29, Guidelines on Consent under Regulation 2016/679, WP 259, p. 7.
[viii] WP29 Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, WP 217, p. 16-17.
[ix] Ibid, p. 16.
[x] Voigt, P., von dem Bussche, A., The EU General Data Protection Regulation (GDPR) – A Practical Guide, Springer International Publishing (2017), p. 102.
[xi] European Data Protection. Law and Practice, Executive Editor: Edurado Ustaran, CIPP/E, Partner, Hogan Lovells, IAPP (2018), p. 118
[xii] WP29 Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, WP 217, p. 16.
[xiii] Ibid, p. 20.
[xiv] Boardman, R., Mullock, J., Mole, A. Bird & Bird Guide to General Data Protection Regulation (2016), p. 10.
[xv] WP29 Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, WP 217, p. 19.
[xvi] Ibid, p. 19.
[xvii] Ibid, p. 20.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

[xviii] Ibid, p. 19.
[xix] Ibid, p. 20.
[xx] European Data Protection. Law and Practice, Executive Editor: Edurado Ustaran, CIPP/E, Partner, Hogan Lovells, IAPP (2018), p. 119.
[xxi] WP29 Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, WP 217, p. 20-21.
[xxii] Ibid, p. 21.
[xxiii] Ibid, p. 21.
[xxiv] European Data Protection. Law and Practice, Executive Editor: Edurado Ustaran, CIPP/E, Partner, Hogan Lovells, IAPP (2018), p. 119.
[xxv] WP29 Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, WP 217, p. 23.
[xxvi] European Data Protection. Law and Practice, Executive Editor: Edurado Ustaran, CIPP/E, Partner, Hogan Lovells, IAPP (2018), p. 119.
[xxvii] WP29 Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, WP 217, p. 24.
[xxviii] Ibid, p. 33.
[xxix] European Data Protection. Law and Practice, Executive Editor: Edurado Ustaran, CIPP/E, Partner, Hogan Lovells, IAPP (2018), p. 122.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

ProLegis

Processing of Special Categories of Personal Data

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

ProLegis

Contents

1. LEGAL FRAMEWORK 4

1.1. Charter of Fundamental Rights of EU 4

1.2. GDPR 4

2. SPECIAL CATEGORIES PERSONAL DATA UNDER GDPR 9

2.1. The logic behind defining certain categories of personal data as special 9

2.2. Types of special categories personal data 10

2.3. Personal data relating to criminal convictions and offences 12

3. LEGAL GROUNDS FOR PROCESSING OF SPECIAL CATEGORIES OF PERSONAL DATA 12

3.1. Explicit consent 13

3.2. Obligations/ specific rights in the field of employment, social security and social protection law 13

3.3. Vital interests of the data subject or of another natural person 14

3.4. Processing by not-for-profit body with a political, philosophical, religious or trade union aim 14

3.5. The data are manifestly made public by the data subject 14

3.6. Establishment, exercise or defense of legal claims/ courts acting in their judicial capacity 15

3.7. Substantial public interest on the basis of EU or Member State law 15

3.8. Preventive or occupational medicine, assessment of the working capacity of the employee, medical diagnosis, provision of health or social care or treatment 16

3.9. Public interest in the area of public health 16

3.10. Processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes 16

3.11. Further conditions in Member State law 17

4. CONCLUSION & PRACTICAL ADVICES 17

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

5. EXTERNAL SOURCES & WEBLINKS 17
Books 17
Documents of the Article 29 Working Party 18
Web Links 18
6. REFERENCES 18

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

1. LEGAL FRAMEWORK

1.1. Charter of Fundamental Rights of EU

Article 8

Protection of personal data

1. Everyone has the right to the protection of personal data concerning him or her.

2. Such data must be processed fairly for specified purposes and ***on the basis of the consent of the person concerned or some other legitimate basis laid down by law****. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.*

3. Compliance with these rules shall be subject to control by an independent authority.

1.2. GDPR

Recital (51)

Personal data which are, by their nature, particularly sensitive in relation to fundamental rights and freedoms merit specific protection as the context of their processing could create significant risks to the fundamental rights and freedoms. Those personal data should include personal data revealing racial or ethnic origin, whereby the use of the term 'racial origin' in this Regulation does not imply an acceptance by the Union of theories which attempt to determine the existence of separate human races. The processing of photographs should not systematically be considered to be processing of special categories of personal data as they are covered by the definition of biometric data only when processed through a specific technical means allowing the unique identification or authentication of a natural person. Such personal data should not be processed, unless processing is allowed in specific cases set out in this Regulation, taking into account that Member States law may lay down specific provisions on data protection in order to adapt the application of the rules of this Regulation for compliance with a legal obligation or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. In addition to the specific requirements for such processing, the general principles and other rules of this Regulation should apply, in particular as regards the conditions for lawful processing. Derogations from the general prohibition for processing such special categories of personal data should be explicitly

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

provided, inter alia, where the data subject gives his or her explicit consent or in respect of specific needs in particular where the processing is carried out in the course of legitimate activities by certain associations or foundations the purpose of which is to permit the exercise of fundamental freedoms.

Recital (52)

Derogating from the prohibition on processing special categories of personal data should also be allowed when provided for in Union or Member State law and subject to suitable safeguards, so as to protect personal data and other fundamental rights, where it is in the public interest to do so, in particular processing personal data in the field of employment law, social protection law including pensions and for health security, monitoring and alert purposes, the prevention or control of communicable diseases and other serious threats to health. Such a derogation may be made for health purposes, including public health and the management of health-care services, especially in order to ensure the quality and cost-effectiveness of the procedures used for settling claims for benefits and services in the health insurance system, or for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes. A derogation should also allow the processing of such personal data where necessary for the establishment, exercise or defence of legal claims, whether in court proceedings or in an administrative or out-of-court procedure.

Recital (53)

Special categories of personal data which merit higher protection should be processed for health-related purposes only where necessary to achieve those purposes for the benefit of natural persons and society as a whole, in particular in the context of the management of health or social care services and systems, including processing by the management and central national health authorities of such data for the purpose of quality control, management information and the general national and local supervision of the health or social care system, and ensuring continuity of health or social care and cross-border healthcare or health security, monitoring and alert purposes, or for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, based on Union or Member State law which has to meet an objective of public interest, as well as for studies conducted in the public interest in the area of public health. Therefore, this Regulation should provide for harmonised conditions for the processing of special categories of personal data concerning health, in respect of specific needs, in particular where the processing of such data is carried out for certain health-related purposes by persons subject to a legal obligation of professional secrecy. Union or

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

Member State law should provide for specific and suitable measures so as to protect the fundamental rights and the personal data of natural persons. Member States should be allowed to maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health. However, this should not hamper the free flow of personal data within the Union when those conditions apply to cross-border processing of such data.

Recital (54)

The processing of special categories of personal data may be necessary for reasons of public interest in the areas of public health without consent of the data subject. Such processing should be subject to suitable and specific measures so as to protect the rights and freedoms of natural persons. In that context, 'public health' should be interpreted as defined in Regulation (EC) No 1338/2008 of the European Parliament and of the Council, namely all elements related to health, namely health status, including morbidity and disability, the determinants having an effect on that health status, health care needs, resources allocated to health care, the provision of, and universal access to, health care as well as health care expenditure and financing, and the causes of mortality. Such processing of data concerning health for reasons of public interest should not result in personal data being processed for other purposes by third parties such as employers or insurance and banking companies.

Recital (55)

Moreover, the processing of personal data by official authorities for the purpose of achieving the aims, laid down by constitutional law or by international public law, of officially recognised religious associations, is carried out on grounds of public interest.

Recital (56)

Where in the course of electoral activities, the operation of the democratic system in a Member State requires that political parties compile personal data on people's political opinions, the processing of such data may be permitted for reasons of public interest, provided that appropriate safeguards are established.

Article 4

Definitions

For the purposes of this Regulation:

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

[…]

(13) ***'genetic data'*** *means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question;*

(14) ***'biometric data'*** *means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data;*

(15) ***'data concerning health'*** *means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status;*

Article 9

Processing of special categories of personal data

1. **Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited**.

2. **Paragraph 1 shall not apply** if one of the following applies:

(a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;

(b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

(c) processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;

(d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;

(e) processing relates to personal data which are manifestly made public by the data subject;

(f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;

(g) processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;

(h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;

(i) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;

(j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

3. Personal data referred to in paragraph 1 may be processed for the purposes referred to in point (h) of paragraph 2 when those data are processed by or under the responsibility of a professional subject to the obligation of professional secrecy under Union or Member State law or rules established by national competent bodies or by another person also subject to an obligation of secrecy under Union or Member State law or rules established by national competent bodies.

4. Member States may maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health.

Article 10

Processing of personal data relating to criminal convictions and offences

Processing of personal data relating to criminal convictions and offences or related security measures *based on Article 6(1) shall be carried out* ***only under the control of official authority or when the processing is authorised by Union or Member State law*** *providing for appropriate safeguards for the rights and freedoms of data subjects. Any comprehensive register of criminal convictions shall be kept only under the control of official authority.*

2. SPECIAL CATEGORIES PERSONAL DATA UNDER GDPR

2.1. The logic behind defining certain categories of personal data as special

Even in the course of drafting the first EU legal act devoted to personal data protection – Directive 95/46 – the European Commission highlighted that the processing of certain categories of personal data could entail higher risk for the fundamental rights and freedoms of the European citizens[i]. Thus, a general prohibition was established for the processing of such 'risky' categories of personal data. They were called 'special categories of personal data', but in practice they were also called 'sensitive data' due to their sensitive nature for the private sphere of the individual[ii]. Such data could be processed only in exceptional circumstances, exhaustively listed in the data protection legislation of the Member States.

GDPR continues this approach but broadens the scope of the special categories personal data and provides for some new exceptions (legal grounds) which entitle the controllers to process such data.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

It should be mentioned that different types of data have different impact of the individuals. Which data are defined as sensitive is based on an objective and not on a subjective principle. In other words, somebody might feel that the data related to their financial status, history of disciplinary sanctions or the Unique Identification Number/ Social Security Number are sensitive. Still, if such data are not recognized by the European legislator as sensitive, they would not fall within the special regime for processing such data irrespective of their sensitive nature from subjective point of view.

In the doctrine, it is indicated that the choice which categories of personal data to be defined as special was substantially influenced by anti-discrimination laws, which explains why data such as Social Security Numbers and credit card details (which if misused could cause serious harm to the individuals) are not defined as sensitive[iii].

2.2. Types of special categories personal data

According to Art. 9, Para 1 of GDPR, the following types of personal data are special category (sensitive data):

- **Personal data revealing racial or ethnic origin** = these categories of personal data are defined as sensitive, as they entail high risk of discrimination. In the legal doctrine, the following examples are given as to what data could fall within this category: person's first name and surname, place of birth, native language or the names of his parents that might, when combined, allow conclusions as to his/ her origin[iv];
- **Political opinions** = these data merit special protection, because they are related to the guarantee of the citizens to form opinions regarding politics and ultimately to participate (actively as politicians and/or passively as electorate and members of civil society) in the political life of the country. Examples of such data include information regarding political party memberships, information regarding joining any petitions, participation in demonstrations, political reunion or similar events, information regarding the support of a certain political idea or its rejection[v]
- **Religious or philosophical beliefs** = these categories of data are tightly related to the freedom of conscience, i.e. the freedom to decide whether to believe in transcendental forces that predetermine our every-day life and whether to manifest it or not. The history of mankind is full of examples where violence has occurred on the basis of religious differences, thus, such data should also be specially protected under the data protection laws;
- **Trade union membership** = information regarding such memberships is sensitive, because it creates the risk of discriminatory treatment in the area of employment law. The European Citizens have the freedom to collective bargaining

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

and action, and thus, should not be unequally treated on the basis of their trade union affiliation[vi];

- **Genetic data** = new category introduced by GDPR as sensitive data. GDPR defines it as 'data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question'. Some Member States have already granted the status of sensitive of this type of data[vii], but GDPR for first time introduces it on EU level. Genetic data should be protected, because such types of data relate not only to the respective data subject but could also potentially affect undefined circle of individuals that are part of the subject's pedigree (including data of death people, data of children, etc.). Moreover, the detailed analysis of such data could reveal other types of sensitive information such as psychological or health data (e.g. predisposition to diseases, vulnerability, etc.);
- **Biometric data for the purpose of uniquely identifying a natural person =** such types of data merit protection, because they enable the controllers unambiguously to identify a given natural person on the basis of their physical or behavioral characteristics: fingerprints, facial recognition, iris, retina, vascular models, DNA, speech, signature, keyboard interaction, etc.). As the processing of such types of data becomes more and more common with the introduction of various technological decisions (e.g. systems for access control to premises, systems for identification on remote devices such as cell phones, tablets, etc.), such processing should be more restrictive and controlled and these factors justify the inclusion of these data in the list of 'sensitive' data under GDPR. Contrary to the practices established in some Member States, the processing of photographs will not automatically be considered as sensitive processing. Photographs will be deemed sensitive data only if they allow the unique identification or authentication of an individual as a biometric (e.g. in an electronic passport or other type of ID document)[viii];
- **Data concerning health or data concerning a natural person's sex life or sexual orientation** = such data is very sensitive, as it interferes within the most intimate aspects of the individual's life. Moreover, the information regarding sex life and sexual orientation entails the risk of discrimination, manipulation, etc. In the theory it is indicated that these data also include the exact identity of an individual's partner(s)[ix]

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

2.3. Personal data relating to criminal convictions and offences

Personal data relating to criminal convictions and offences or related security measures are **not** proclaimed as a special category of personal data. Still, the legislation of some Member States treats them as sensitive[x]. Nonetheless, such types of information also entail the risk of unequal treatment (e.g. in the area of employment), thus, these data are also subject to special rules for processing. GDPR does not introduce significant amendment with respect to the old Directive 95/46 in relation to criminal convictions and offences data. In the same time, given the fact the rules of the Directive were transposed in different ways in the Member State, GDPR would introduce a more general approach on EU level towards such data. According to the wording of Art. 10 of GDPR, these data could be processed on the basis of one of the grounds of Art. 6 provided that one of two **alternative** additional conditions is met:

(i) The processing should be under the control of official authority, or
(ii) The processing is authorized by EU/ Member State law providing for appropriate safeguards for the rights and freedoms of data subjects.

There is uncertainty surrounding this provision, because it is unclear how these two additional requirements specified thereto apply together with Art. 6. The conservative interpretation is that private or commercial entities could not process such data, in other words 'there is no room in the Regulation for private or commercial processing of this data'[xi]. The other interpretation is that such type of data could be processed under all the possible legal grounds provided that the additional conditions (under the control of official authority or if permitted under the applicable law) are met. In the doctrine it is indicated that this provision would likely lead to continued national divergence[xii]. Although the local authorities (LAs) will act as public authorities and theoretically could justify the first additional requirement for processing (under the control of official authority), it would still be advisable to carefully examine the local regulations when such types of data could be processed (especially in the context of HR activities and collection of criminal records, as the respective LA acts as an employer in such context rather than as a public power holder and the applicability of the fist additional condition is questionable).

3. LEGAL GROUNDS FOR PROCESSING OF SPECIAL CATEGORIES OF PERSONAL DATA

The general prohibition for processing special categories of personal data does not apply, provided that one of the **alternative** conditions listed below is fulfilled:

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

3.1. Explicit consent

The requirements that must be met under GDPR in order to have valid consent (freely given, specific, informed, unambiguous) apply in any case for processing of special categories personal data. The element 'explicit' is not defined under GDPR. Article 29 Working Party (WP29) has indicated that explicit consent is required in situations where serious data protection risk emerge, and a high level of individual control over personal data is appropriate[xiii].

The term 'explicit' refers to the way consent is expressed by the data subject – the data subject must give an express statement of consent[xiv]. One of the ways to give consent is to expressly confirm it in written statement. In online context, various solutions could be applied by filling in an electronic form, by sending an email, by uploading a scanned document with the signature of the data subject, or by using an electronic signature. Any other means which would enable the controller to demonstrate the high threshold for the way the consent must be given would be appropriate.

Given the imbalance of powers between the data subjects and the public authorities, it is not advisable for the LAs to rely predominantly on explicit consent for processing of special categories of personal data (including in the relations with citizens and employees).

3.2. Obligations/ specific rights in the field of employment, social security and social protection law

This condition is especially relevant for LAs when managing their internal HR process. Processing of special categories of personal data might be necessary at every stage of the labor relation – from its arising (the process of hiring new personnel), through its performance and amendment and ultimately to its termination.

Examples where such processing might be necessary include the administration of sick leaves and maternity leaves; transferring the employee to a more appropriate position due to health considerations upon request by the healthcare authorities; complying with mandatory rules that provide for special protection of certain categories of employees in case of termination of the labor relationship, etc.

The general requirements introduced in GDPR for the applications of this ground are:

(i) The processing must be necessary to perform an obligation of the data controller or a certain right of the data subject;
(ii) This obligation/ right could be provided in EU/ Member State law or in a collective (bargaining) agreement;

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

(iii) There should be appropriate safeguards for the fundamental rights and the interests of the data subject.

In order to apply this legal ground, the specific national legislation in the respective Member State law where the LA operates as an employer, needs to be observed. As the employment law is one of the areas where GDPR authorizes the Member States to adopt additional legislation with respect to personal data protection (Art. 88), a local-based approach is advisable for LAs when applying this ground.

3.3. Vital interests of the data subject or of another natural person

Similar to the legal ground under Art. 6, Para 1, item 'd' of GDPR, such situation refers to circumstances of life or death[xv]. The vital interest could be either of the data subject or of another person. What is different in comparison to Art. 6 is that the controller bears the burden to demonstrate the presence of an additional condition, namely that 'the data subject is physically or legally incapable of giving consent'. This wording implies that the controller should try to obtain the consent of the data subject first[xvi].

3.4. Processing by not-for-profit body with a political, philosophical, religious or trade union aim

The possibility to process sensitive data under this legal ground is provided for certain non-profit organization such as political parties, foundations, churches, other forms of philosophical, religious or trade union organizations. Such organizations could process sensitive data if:

(i) these data relate solely to the members/ to former members of the body or to persons who have regular contact with it;
(ii) the processing is in the course of their legitimate activities;
(iii) the processing takes place in connection with their specific purposes;
(iv) there are appropriate safeguards for the data subject's rights;
(v) the personal data are not disclosed outside that body without the consent of the data subjects.

Other specific requirements should be sought in national law[xvii].

This legal ground would have almost no practical application for LAs in the course of their activity.

3.5. The data are manifestly made public by the data subject

If the personal data are manifestly disclosed to the general public by the data subject, then it is presumed that the data subject has waived the special protection granted to

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

such information. In any case, the decision to disclose such information needs to be result of the individual's free choice[xviii]. Such disclosure may take different forms – data from publicly accessible registers, websites, lists, forums or even from a profile in a social network that is accessible without a user account, etc.[xix] In any case, the fact that such data are manifestly made public does not release the controller from the obligation to comply with the other requirements under the GDPR – e.g. compliance with the data protection principles, observing the data protection by default & data protection by design, taking appropriate measures to guarantee the security of the data, etc.

3.6. Establishment, exercise or defense of legal claims/ courts acting in their judicial capacity

In certain cases, processing of sensitive data might be necessary for a controller to establish, exercise or defend legal claims. The controller bears the burden to prove that there is a necessity for such processing, i.e. that there is a close and substantive connection between the processing and the purposes[xx]. Such situations might include e.g. appeals before administrative courts of acts issued by the LAs where processing of sensitive data took place in the preceding administrative procedure; labor disputes where the health data of the employees should have been taken into account by the LA as an employer, etc.

Further to that, the processing within the judicial activities of courts could also substantiate processing of such categories of personal data.

3.7. Substantial public interest on the basis of EU or Member State law

This provision of GDPR authorizes Member States to introduce in their national legislation specific hypothesis where sensitive data could be processed justifying such processing with substantial public interest.

In any case, to meet the requirements of GDPR, the Member States must ensure that:

(i) the processing should be proportionate to the aim pursued;
(ii) the essence of the right to data protection is respected;
(iii) the legislation adopted provides for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

It remains to be seen how this opportunity would be used in future. A case by case analysis of the respective local law is advisable for LAs in order to determine whether they can rely on such ground.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

3.8. Preventive or occupational medicine, assessment of the working capacity of the employee, medical diagnosis, provision of health or social care or treatment

The prohibition to process special categories of personal data does not apply to processing for medical/ social care purposes[xxi]. Such processing might take place in various areas such as occupational medicine, medical diagnosis, or provision of services in the area of social or medical care. Such processing might take place either on the basis of EU/ Member State law or under a contract with health care professional[xxii]. Further to that, Art. 9, Para 3 of GDPR enables processing of sensitive data by a person bound under obligation for professional secrecy.

This legal ground applies to doctors, nurses and other persons involved in the provision of healthcare services[xxiii].

From practical point of view, this provision would enable LAs in their capacity of employers to ensure occupational medicine services as part of the bigger obligation to ensure health and safety working conditions.

3.9. Public interest in the area of public health

According to Recital 54 of GDPR, 'public health' should be interpreted in accordance with the definition of Regulation (EC) No 1338/2008, namely all elements related to health, health status, including morbidity and disability, the determinants having an effect on that health status, health care needs, resources allocated to health care, the provision of, and universal access to, health care as well as health care expenditure and financing, and the causes of mortality.

Reasons that could justify the application of this legal ground could be the protection against serious cross-border threats to health or ensuring high standards of quality and safety of health care, medical products or medical devices[xxiv].

The processing of health data for reasons of public interest should not result in personal data being processed for other purposes by third parties such as employers or insurance and banking companies.

3.10. Processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes

The processing for such purposes should be based on Member State/ EU law. GDPR requires that the legislative provisions enabling such processing should be: proportionate

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject. The safeguards introduced must correspond to the sensitive nature of the personal data concerned[xxv].

3.11. Further conditions in Member State law

Art. 9, Para 4 of GDPR authorizes the Member States to introduce further conditions or limitations for processing of certain special categories of personal data, namely: genetic data, biometric data or data concerning health. Thus, local legislation applicable to LA should be monitored in future.

4. CONCLUSION & PRACTICAL ADVICES

The LAs should be aware that certain categories of personal data merit special protection, because they are inherently related with the most intimate private spheres and/ or entail the risk of discrimination. By general rule, processing of such data is prohibited, unless additional conditions (exceptions of this rule) are present.

The most practical aspects which might affect LAs' activities are the processing activities of employees health data. GDPR permits such processing, but only if necessary for controller's obligation (or right of the data subject) under the employment law.

The data regarding criminal convictions and offences are not special category, but also are under special regime under GDPR. The HR practices for collecting criminal records or making extensive background checks of future employees should be revised in the light of GDPR.

5. EXTERNAL SOURCES & WEBLINKS

Books

- **Boardman, R., Mullock, J., Mole, A.** Bird & Bird Guide to General Data Protection Regulation (2016);
- **Ehmann, E., Helfrich, M.** EG Datenschutzrichtlinie: Kurzkommentar, Verlag Dr. Otto Schmidt, Koln, (1999)
- **Voigt, P., von dem Bussche, A.**, The EU General Data Protection Regulation (GDPR) – A Practical Guide, Springer International Publishing (2017);
- **EU** General Data Protection Regulation (GDPR). An Implementation and Compliance Guide, IT Governance Publishing, Cambridgeshire (2016);

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

- **European** Data Protection. Law and Practice, Executive Editor: Edurado Ustaran, CIPP/E, Partner, Hogan Lovells, IAPP (2018);

Documents of the Article 29 Working Party

- WP29, Guidelines on Consent under Regulation 2016/679, WP 259;
- WP29, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, WP 217;

Web Links

- http://europa.eu/rapid/press-release_IP-18-386_en.htm
- https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en
- https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/sensitive-data/what-personal-data-considered-sensitive_en
- https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/sensitive-data/under-what-conditions-can-my-company-organisation-process-sensitive-data_en

6. REFERENCES

[i] Ehmann, E., Helfrich, M. EG Datenschutzrichtlinie: Kurzkommentar, Verlag Dr. Otto Schmidt, Koln, (1999), p. 130-131.
[ii] GDPR explicitly recognizes the term 'sensitive data' – see e.g. Recital 10.
[iii] European Data Protection. Law and Practice, Executive Editor: Edurado Ustaran, CIPP/E, Partner, Hogan Lovells, IAPP (2018), p. 123.
[iv] Voigt, P., von dem Bussche, A., The EU General Data Protection Regulation (GDPR) – A Practical Guide, Springer International Publishing (2017), p. 111.
[v] Ibid, p. 111.
[vi] Ibid, p. 111.
[vii] In Bulgaria such data are sensitive since 2005.
[viii] Boardman, R., Mullock, J., Mole, A. Bird & Bird Guide to General Data Protection Regulation (2016), p. 18.
[ix] Voigt, P., von dem Bussche, A., The EU General Data Protection Regulation (GDPR) – A Practical Guide, Springer International Publishing (2017), p. 111.
[x] Boardman, R., Mullock, J., Mole, A. Bird & Bird Guide to General Data Protection Regulation (2016), p. 19.
[xi] EU General Data Protection Regulation (GDPR). An Implementation and Compliance Guide, IT Governance Publishing, Cambridgeshire (2016), p. 196.
[xii] Boardman, R., Mullock, J., Mole, A. Bird & Bird Guide to General Data Protection Regulation (2016), p. 19.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

[xiii] WP29, Guidelines on Consent under Regulation 2016/679, WP 259, p. 18.
[xiv] Ibid, p. 18.
[xv] European Data Protection. Law and Practice, Executive Editor: Edurado Ustaran, CIPP/E, Partner, Hogan Lovells, IAPP (2018), p. 126.
[xvi] Ibid, p. 126.
[xvii] Ibid, p. 126-127.
[xviii] Voigt, P., von dem Bussche, A., The EU General Data Protection Regulation (GDPR) – A Practical Guide, Springer International Publishing (2017), p. 113.
[xix] Ibid, p. 113.
[xx] European Data Protection. Law and Practice, Executive Editor: Edurado Ustaran, CIPP/E, Partner, Hogan Lovells, IAPP (2018), p. 127.
[xxi] Ibid, p. 128.
[xxii] Ibid, p. 129.
[xxiii] Ibid, p. 129.
[xxiv] Voigt, P., von dem Bussche, A., The EU General Data Protection Regulation (GDPR) – A Practical Guide, Springer International Publishing (2017), p. 114.
[xxv] Ibid, p. 115.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

ProLegis

Designation, Position and Tasks of Data Protection Officers (DPOs)

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

ProLegis

Contents

1. LEGAL FRAMEWORK 4

GDPR 4

2. DESIGNATION OF THE DPO 7

2.1. Mandatory appointment under GDPR 7

2.1.1. Public authority or body 7

2.1.2. The core activities of the controller/ processor […] require regular and systematic monitoring of data subjects on a large scale 7

2.1.3. The core activities of the controller/ processor consist of processing on a large scale of special categories of data […] and personal data relating to criminal convictions and offences 9

2.2. Other situations for appointing DPO 9

2.2.1. Mandatory appointment under EU/ Member State law 9

2.2.2. Voluntary appointment 10

2.3. Contractual relations with the DPO 10

2.3.1. Labour contract 10

2.3.2. Service contract 10

3. POSITION OF THE DPO 11

3.1. Involvement in all issues related to personal data protection 11

3.2. Ensuring necessary resources and independence 11

3.3. Conflict of interest 13

4. TASKS OF THE DPO 13

4.1. Monitoring 13

4.2. DPIA 14

4.3. Contact point 14

4.4. Record keeping 14

5. CONCLUSION & PRACTICAL ADVICES 15

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

6. EXTERNAL SOURCES & WEBLINKS 16
Books 16
Documents of the Article 29 Working Party 16
Web Links 16
7. REFERENCES 16

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

1. LEGAL FRAMEWORK

GDPR

Recital (97)

Where the processing is carried out by a public authority, except for courts or independent judicial authorities when acting in their judicial capacity, where, in the private sector, processing is carried out by a controller whose core activities consist of processing operations that require regular and systematic monitoring of the data subjects on a large scale, or where the core activities of the controller or the processor consist of processing on a large scale of special categories of personal data and data relating to criminal convictions and offences, a person with expert knowledge of data protection law and practices should assist the controller or processor to monitor internal compliance with this Regulation. In the private sector, the core activities of a controller relate to its primary activities and do not relate to the processing of personal data as ancillary activities. The necessary level of expert knowledge should be determined in particular according to the data processing operations carried out and the protection required for the personal data processed by the controller or the processor. Such data protection officers, whether or not they are an employee of the controller, should be in a position to perform their duties and tasks in an independent manner.

Article 37

Designation of the data protection officer

1. The controller and the processor shall designate a data protection officer in any case where:

(a) the processing is carried out by a public authority or body, except for courts acting in their judicial capacity;

(b) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

(c) the core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 9 and personal data relating to criminal convictions and offences referred to in Article 10.

2. A group of undertakings may appoint a single data protection officer provided that a data protection officer is easily accessible from each establishment.

3. Where the controller or the processor is a public authority or body, a single data protection officer may be designated for several such authorities or bodies, taking account of their organisational structure and size.

4. In cases other than those referred to in paragraph 1, the controller or processor or associations and other bodies representing categories of controllers or processors may or, where required by Union or Member State law shall, designate a data protection officer. The data protection officer may act for such associations and other bodies representing controllers or processors.

5. The data protection officer shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the tasks referred to in Article 39.

6. The data protection officer may be a staff member of the controller or processor, or fulfil the tasks on the basis of a service contract.

7. The controller or the processor shall publish the contact details of the data protection officer and communicate them to the supervisory authority.

Article 38

Position of the data protection officer

1. The controller and the processor shall ensure that the data protection officer is involved, properly and in a timely manner, in all issues which relate to the protection of personal data.

2. The controller and processor shall support the data protection officer in performing the tasks referred to in Article 39 by providing resources necessary to carry out those tasks and access to personal data and processing operations, and to maintain his or her expert knowledge.

3. The controller and processor shall ensure that the data protection officer does not receive any instructions regarding the exercise of those tasks. He or she shall not be

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

dismissed or penalised by the controller or the processor for performing his tasks. The data protection officer shall directly report to the highest management level of the controller or the processor.

4. Data subjects may contact the data protection officer with regard to all issues related to processing of their personal data and to the exercise of their rights under this Regulation.

5. The data protection officer shall be bound by secrecy or confidentiality concerning the performance of his or her tasks, in accordance with Union or Member State law.

6. The data protection officer may fulfil other tasks and duties. The controller or processor shall ensure that any such tasks and duties do not result in a conflict of interests.

Article 39

Tasks of the data protection officer

1. The data protection officer shall have at least the following tasks:

(a) to inform and advise the controller or the processor and the employees who carry out processing of their obligations pursuant to this Regulation and to other Union or Member State data protection provisions;

(b) to monitor compliance with this Regulation, with other Union or Member State data protection provisions and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;

(c) to provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to Article 35;

(d) to cooperate with the supervisory authority;

(e) to act as the contact point for the supervisory authority on issues relating to processing, including the prior consultation referred to in Article 36, and to consult, where appropriate, with regard to any other matter.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

2. The data protection officer shall in the performance of his or her tasks have due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing.

2. DESIGNATION OF THE DPO

2.1. Mandatory appointment under GDPR

2.1.1. Public authority or body

GDPR does not contain a legal definition what is understood under "public authority or body". Whether certain natural/ legal person constitutes public authority/ body should be defined according to the national legislation of each respective Member State. This concept should be interpreted **broadly** and, in any case, includes national, regional and **local authorities**. According to WP29, however, it may also include certain natural/ legal persons whose activities are governed by public/ private law (e.g. public transport services, water and energy supply, road infrastructure, public service broadcasting, public housing or disciplinary bodies for regulated profession)[i]. The logic behind such an interpretation is that the citizens (data subjects) have limited choice whether and how their personal data will be processed by such entities. Although such interpretation is not mandatory and binding, a careful consideration and analysis within these organizations whether to appoint a DPO is recommendable.

It should be noted that WP29 recommends as a good practice to designate a DPO whose functions should also cover all processing operations carried out, including those that are not related to the performance of a public task or exercise of official duty (e.g. the relations with the employees)[ii]. However, none of the provisions of GDPR require the appointment of DPO merely for the processing activities related to public functions. Thus, the more reasonable and safe interpretation is that LA shall appoint DPO **who is responsible for all data processing activities** within the organization (relations with citizens, employees, candidates for work, ex-employees, other public authorities, etc.).

2.1.2. The core activities of the controller/ processor […] require regular and systematic monitoring of data subjects on a large scale

The data processing activities of LA would generally fall within the scope of item 2.1.1. above, i.e. LA should appoint DPO on the basis of their capacity of public authority/ body. For the sake of clarity, below will be made a brief analysis of the two other hypothesis under GDPR when the appointment of DPO shall be mandatory. This information might

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

be useful for private entities whose capital is partly or wholly owned by the municipality or other LA/ state bodies and who do not fall within the scope of “public authority/ body”.

Under the term **“core activities”** one should understand the key operations necessary to achieve the controller’s or processor’s goals[iii]. Examples given by WP29 include the processing of health records within hospitals or surveillance conducted by private security company. In the same time, standard IT support activities are excluded from the “core activities” of the organization[iv].

The concept **“large scale”** is not explicitly defined in GDPR. It is explicitly mentioned that processing at regional, national or supranational level which includes considerable amount of data and which could affect a large number of data subjects and which are likely to result in a high risk could be deemed processing on a “large scale”. To the contrary, sole-practitioners such as a single healthcare specialists or lawyers do not process personal data on a “large scale”.

According to WP29, a non-exhaustive list of activities which could be deemed large-scale processing include:

- processing of patient data by a hospital;
- processing of travel data of individuals using a city’s public transport system (e.g. tracking via travel cards);
- processing of real time geo-location data of customers of an international fast food chain for statistical purposes by a processor specialised in providing these services;
- processing of customer data by an insurance company/ a bank;
- processing of personal data for behavioural advertising by a search engine
- processing of data (content, traffic, location) by telephone or internet service providers[v].

The concept **“regular”** is inherently linked with processing that takes place either permanently (constantly) or periodically. The concept **“systematic monitoring”** requires the processing to take place upon a certain plan, strategy or similar pre-defined methodology, in an organized manner, within a system[vi]. Examples include inter alia operating telecommunication network, profiling, behavioural advertising, processing information from smart devices, etc.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union’s Rights, Equality and Citizenship Programme (2014-2020).

2.1.3. The core activities of the controller/ processor consist of processing on a large scale of special categories of data […] and personal data relating to criminal convictions and offences

For the terms “core activities” and “large scale” see item 2.1.2. above.

The term and should be interpreted correctively as “or”. In other words, any processing which includes **either** the processing of special categories of data **or** personal data relating to criminal convictions and offences which is on a large scale and is part of the core activity of the organization should require the designation of DPO.

Special categories of data are:

- personal data revealing racial or ethnic origin;
- political opinions;
- religious or philosophical beliefs;
- trade union membership;
- genetic data;
- biometric data for the purpose of uniquely identifying a natural person:
- data concerning health or data concerning a natural person's sex life or sexual orientation.

Personal data relating to criminal convictions and offences may include information contained in court judgements, criminal records, acts of investigatory bodies.

2.2. Other situations for appointing DPO

2.2.1. Mandatory appointment under EU/ Member State law

Pursuant to Art. 37 (4) of GDPR, EU and/or Member States are entitled to provide for other situations where the appointing of DPO shall be mandatory. Such mandatory appointment might be required by qualitative sign (e.g. for certain sector-specific processing activities) or by quantitative sign (e.g. in case the organization processes the personal data of certain number data subjects). Germany for example has introduced in its local data protection legislation broader requirements than GDPR: (i) companies doing business in Germany and engaging at least 10 persons in the field of automated processing will be obliged to appoint a DPO; (ii) in cases of automated processing in the course of business for the purpose of a transfer of an anonymized transfer or of market or opinion research, companies must appoint a DPO regardless of the number of persons employed for the automated processing of personal data[vii].

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

2.2.2. Voluntary appointment

GDPR also provides for the possibility voluntarily to appoint DPO. Such an approach might be reasonable for organizations who are eager to demonstrate compliance with the data protection rules and to foster transparency and trust. Since the activity of the LAs would rather fall within the first mandatory requirement (public authority/ body), the voluntary appointment might be applied for certain organizations whose capital is owned by the municipality/ the state – e.g. public transport enterprises, public schools/ universities, public providers of utilities (water-, gas-, electricity supply), etc.

2.3. Contractual relations with the DPO

2.3.1. Labour contract

GDPR explicitly provides for the opportunity to appoint the DPO on the basis of a labour contract. This implies two possibilities: (i) to appoint somebody already working in the organization to combine their function with the functions of the DPO, or (ii) to reveal a new working position for the DPO. The choice between these two possibilities depends pretty much on the structure, number of employees, workload and type and number of the data processing activities and should be made on case by case basis. If the respective LA's organization is rather small (e.g. is located in a small village with limited number of citizens whose data are processed) it might be reasonable not to appoint a new staff member, but rather to allocate the DPO's function to somebody already working in the organization (in any case conflict of interest should be avoided). To the contrary, if the LA's organization is huge and/ or its everyday activities are related to the processing of significant amounts of personal data (or sensitive data/ data related to convictions and criminal offences), the choice to open a new position for (at least) one DPO would seem justified.

2.3.2. Service contract

GDPR does not oblige the organizations to appoint the DPOs only as staff members. The Regulation explicitly provides that the function of DPO may be outsourced to external individual/ organization under a service contract. WP29 recommends as a good practice for external teams of DPOs to have a designated lead contact and 'person in charge' of every client which should be specified in the service contract[viii]. In addition, each member of the external DPO organization should fulfil all applicable requirements under GDPR.

Outsourcing the DPO functions to external organization could also be reasonable, as such organization would have the necessary level of expert knowledge, experience and to maintain any relevant certifications[ix].

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

Last but not least, depending on the local law, concluding a service contract with an external DPO might require the conducting of certain formal procedures (e.g. under public procurement law).

3. POSITION OF THE DPO

3.1. Involvement in all issues related to personal data protection

GDPR explicitly provides that the DPO should be involved in all issues related to the personal data protection in the organization. WP29 sees the involvement of the DPO (in terms of consultations, advices, control, etc.) in each process that includes personal data processing from the earliest stage possible as one of the tools to ensure privacy by design[x].

Practical implications of the DPOs involvement in the organization could include for example:

- Seeking advice during the conduction of data protection impact assessment (DPIA) (Art. 35, Para 2 of GDPR);
- Participation in work meetings (WP29 prescribes participation in meetings of senior and middle management, but in practice the DPO's interaction with the staff on expert level could have similar (if not higher) added value);
- Seeking consultation from the DPO every time when a management decision regarding data processing shall be taken;
- Seeking consultation from the DPO what measures to be taken if a data breach occurs.

3.2. Ensuring necessary resources and independence

The DPO could not properly perform their function if not provided with the necessary resources. The management of the organization is thus responsible to ensure that the DPO is properly secured at least in terms of:

- **Organizational matters:**
  - The DPO should have a team to support them when performing their functions. This is particularly important for larger organizations. Even the appointment of several DPOs might be the solution in certain cases.
  - Access to all other teams in the organization. The DPO could not exercise properly its functions if they do not interact properly with all other teams responsible for data processing (e.g. Registry Office and File Keeping

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

Department, Legal Department, Human Resources, Accountancy, IT Department, etc.);

- Accountable only before the highest management. GDPR explicitly provides that the DPO should be responsible only to the highest management of the organization. For LAs this could be e.g. the mayor, the municipality council, the director/ chairman of the respective administrative unit, etc. This requirement is very important in terms of ensuring independence of the DPO. If the DPO's connection with the management was indirect (e.g. through intermediaries such as the head of Legal or Human Resources Department), the DPO could not properly exercise their functions, because they will be in situation where the DPO is accountable before somebody over who the DPO should exercise control.
- Time to perform function. This requirement should be observed especially in cases where the DPO is appointed on part-time basis or the external DPO carries out data protection in addition to other duties[xi]. WP29 prescribes as a good practice to establish a percentage of time for the DPO function where it is not performed on a full-time basis.

- **Financial matters**
  - The DPO should have the necessary financial resources to conduct their functions. If the organization does not ensure sufficient budget for data protection activities, the proper exercise of the DPO's functions could be jeopardized.
  - The DPO should have the necessary facilities and equipment (rooms, computers, Internet connectivity, data bases, technical solutions like software programs, etc.)
- **Education matters** – the DPO's level of expert knowledge should be constantly upgraded (through courses, ensuring new literature, etc.). Given the fact that the data protection is a very dynamic area of human knowledge, it is understandable that the DPO should be up-to-date with the latest trends and developments in order to properly ensure the highest level possible in terms of data protection in the organization and to face the newest challenges in terms of technological and legal development.

Important aspect of the DPO's independence is the **prohibition for sanctioning/ causing any unfavourable consequences** to the DPO for performing their tasks. The unfavourable consequences could vary to a wide range of situations – from dismissal or other types of disciplinary penalty to denial from promotion, denial from benefits received by the other employees, etc. It could be expected that the Member States introduce

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

amendments in their labour legislation and provide for protection of the DPOs against dismissal for the time during the performance of their functions and some period thereafter[xii]. In the same time, a reasonable interpolation of this prohibition should be made – the DPO could not be penalized for the duly performance of their services. However, if the DPO lacks the necessary knowledge and skills, conducts disciplinary violations, etc., the organizations should be able to dismiss them on all the grounds for dismissal available in the respective national labour legislation.

3.3. Conflict of interest

If the DPO is designated under a labour contract, this designation should not result in conflict of interest. A conflict of interest could arise if the DPO has another function within the organization which determines the purposes and the means for data processing within given internal process. In other words, the DPO could not be at the same time director, chief executive, chief operating, chief financial, chief medical officer, head of marketing department, head of Human Resources or head of IT departments[xiii]. In addition, other roles lower down in the organizational structure could cause conflict of interest, if such positions or roles lead to the determination of purposes and means of processing (e.g. accountant, legal advisor, IT specialist).

A conflict of interests may arise not only in case of designating DPO under a labour contract, but also in case of external DPO. If the DPO is asked to represent the controller or processor before the courts in cases involving data protection issues, a conflict of interest would arise, because the controller and the processor have contradicting interests.

4. TASKS OF THE DPO

4.1. Monitoring

One of the key tasks of the DPO is to monitor all the data processing activities within the organization. This is inherently connected with receiving/ collecting of information, internal analysis of this information and making clarifications, recommendations and giving advises within the organization. The monitoring function is focused on the internal processes within the organization, thus, informed and advised should be not only the management, but also the regular employees on expert level whose duties are related to processing of personal data.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

4.2. DPIA

GDPR provides that the DPO should be involved in the DPIA with advisory functions. WP29 recommends as a matter of good practice to seek advice from the DPO regarding one or more from the following issues related to the impact assessment:

- whether to carry out a DPIA at all;
- what methodology to follow when carrying out a DPIA;
- whether to carry out the DPIA internally or to outsource it;
- what safeguards (including technical and organizational measures) to apply to mitigate any risks to the rights and interests of the data subjects;
- whether the data protection impact assessment has been correctly carried out and whether its conclusions are in compliance with the GDPR[xiv].

If the management of the organization decides to deviate from the DPO's advices, as part of the accountability principle, it is advisable to have this decision and the reasons thereof documented and to be able to present this documentation to the supervisory authorities in case of an audit.

4.3. Contact point

The DPO is the main point of contact for both the supervisory authorities (Art. 39, Para 1, item "e" of GDPR) and the data subjects (Art. 38, Para 4 of GDPR) regarding any matters related to data protection within the organization. Thus, it is of paramount importance properly to communicate the contact details of the DPO to the supervisory authority and to the data subjects. Moreover, the requirement for providing the DPO's contact details is one of the elements of the transparency principle under Art. 12, 13 and 14 of GDPR.

Nothing in GDPR precludes the DPO from the opportunity to seek advice from the supervisory authorities regarding any issue related to data protection within the organization.

4.4. Record keeping

Although the obligation to keep records of processing activities is provided only for controllers and processors and not for the DPOs, nothing in GDPR precludes organizations from assigning this function to the DPO. The tasks of the DPO listed in the GDPR are only **minimum set**, thus, organizations are free in their discretion to delegate any other tasks to the DPO. WP29 considers the allocation of the recording keeping obligation to the DPO as one of the tools enabling the DPO to perform its tasks of monitoring compliance, informing and advising the controller/ the processor[xv]. As the

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

record is an effective tool for ensuring accountability, it might be reasonable to delegate this obligation to the DPO.

5. CONCLUSION & PRACTICAL ADVICES

The DPO is one of the key figures in ensuring the compliance with the new data protection rules. The importance of this role depends pretty much of the respective organization itself. If the organization properly involves the DPO in all issues related to data protection and ensures the necessary resources for the DPO to conduct their functions, then DPO could be one of the decisive factors for ensuring compliance and fostering trust among the society. If not, the DPO would be a rather illusive figure with no real functions than eventually managing the communication related to data protection, which is not the idea of this role under GDPR.

The LAs should be encouraged to designate qualified DPOs, which given the lack of prepared individuals on EU level could turn out to be a difficult task. In any case, the next few years will predetermine how the role of the DPO will evolve. It would be positive for the society if the LAs are one of the pioneering examples in terms of how best to use the figure of the DPO.

LAW AND INTERNET FOUNDATION
VICESSE
LATVIAN ASSOCIATION OF LOCAL AND REGIONAL GOVERNMENTS
SMA THE EXTENDED ENTERPRISE
SNSPA

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

6. EXTERNAL SOURCES & WEBLINKS

Books

- **Harting, N.** Datenschutz-Grundverordnung: Das neue Datenschutzrecht in der betrieblichen Praxis, Verlag Dr. Otto Schmidt KG, Köln, 2016;
- **Voigt, P., von dem Bussche, A.** The EU General Data Protection Regulation (GDPR) – A Practical Guide, Springer International Publishing (2017);
- **Boardman, R., Mullock, J., Mole, A.** Bird & Bird Guide to General Data Protection Regulation (2016);
- **EU** General Data Protection Regulation (GDPR). An Implementation and Compliance Guide, IT Governance Publishing, Cambridgeshire (2016);

Documents of the Article 29 Working Party

- WP29, Guidelines on Data Protection Officers ('DPOs'), WP 243 rev.01;

Web Links

- http://europa.eu/rapid/press-release_IP-18-386_en.htm
- https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en
- ….

7. REFERENCES

[i] WP29, Guidelines on Data Protection Officers ('DPOs'), WP 243 rev.01, p. 6.
[ii] Ibid.
[iii] Ibid.
[iv] Ibid, p. 6-7.
[v] Ibid, p. 8.
[vi] See the exact interpretation made by WP29 in WP29, Guidelines on Data Protection Officers ('DPOs'), WP 243 rev.01, p. 8.
[vii] Demmel, A. The New German Federal Data Protection Act, Squire Patton Boggs, URL: <https://www.squirepattonboggs.com/~/media/files/insights/publications/2017/09/the-new-german-federal-data-protection-act/27836--german-federal-data-protection-alert.pdf> (26.03.2018);
[viii] WP29, Guidelines on Data Protection Officers ('DPOs'), WP 243 rev.01, p. 22-23.
[ix] EU General Data Protection Regulation (GDPR). An Implementation and Compliance Guide, IT Governance Publishing, Cambridgeshire (2016), p. 58.
[x] WP29, Guidelines on Data Protection Officers ('DPOs'), WP 243 rev.01, p. 13.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

[xi] Ibid, p. 14.

[xii] Germany has already introduced protection for the DPO against dismissal one year after the appointment ends, except for extraordinary termination reasons. See Demmel, A. The New German Federal Data Protection Act, Squire Patton Boggs, URL: <https://www.squirepattonboggs.com/~/media/files/insights/publications/2017/09/the-new-german-federal-data-protection-act/27836--german-federal-data-protection-alert.pdf> (26.03.2018);

[xiii] WP29, Guidelines on Data Protection Officers ('DPOs'), WP 243 rev.01, p. 16.

[xiv] Ibid, p.17.

[xv] WP29, Guidelines on Data Protection Officers ('DPOs'), WP 243 rev.01, p. 19.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

ProLegis

Data Protection Impact Assessment

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

ProLegis

Contents

1. Legal framework 3

1.1. General Data Protection Regulation (GDPR) 3

2. When is a DPIA required? 5

2.1. Basics 5

2.2. Cases where a DPIA is mandatory 6

2.2.1. Further considerations regarding the need to conduct a DPIA 6

2.2.2. Conducting a DPIA for several similar data processing systems 7

2.2.3. Positive and negative lists for DPIA 7

2.3. Timing of DPIA 7

2.4. Review of the DPIA 8

2.5. Consultation with data protection authority pursuant Art 36 GDPR 9

3. Who is responsible to conduct a DPIA? 9

3.1. Basis 9

3.2. Participation in the DPIA 9

4. How to conduct a DPIA 10

4.1. Basis 10

4.2. Implementation of a DPIA 10

4.3. Minimum content of a DPIA 11

4.4. The DPIA Process 12

4.5. Inclusion of data subjects or their representatives 13

4.6. The report on the implementation of a data protection impact assessment 14

5. Conclusions and practical tips 16

6. External Sources & WEBLINKS 17

6.1. Books and Articles 17

6.2. Documents of the Article 29 Working Party 18

6.3. Web Links 18

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

1. Legal framework

1.1. General Data Protection Regulation (GDPR)

Article 35

Data protection impact assessment

1. Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks.

2. The controller shall seek the advice of the data protection officer, where designated, when carrying out a data protection impact assessment.

3. A data protection impact assessment referred to in paragraph 1 shall in particular be required in the case of:

(a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;

(b) processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10; or

(c) a systematic monitoring of a publicly accessible area on a large scale.

4. The supervisory authority shall establish and make public a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment pursuant to paragraph 1. The supervisory authority shall communicate those lists to the Board referred to in Article 68.

5. The supervisory authority may also establish and make public a list of the kind of processing operations for which no data protection impact assessment is required. The supervisory authority shall communicate those lists to the Board.

6. Prior to the adoption of the lists referred to in paragraphs 4 and 5, the competent supervisory authority shall apply the consistency mechanism referred to in Article 63 where such lists involve processing activities which are related to the offering of goods or

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

services to data subjects or to the monitoring of their behaviour in several Member States or may substantially affect the free movement of personal data within the Union.

7. The assessment shall contain at least:

(a) a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;

(b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes;

(c) an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1; and

(d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.

8. Compliance with approved codes of conduct referred to in Article 40 by the relevant controllers or processors shall be taken into due account in assessing the impact of the processing operations performed by such controllers or processors, in particular for the purposes of a data protection impact assessment.

9. Where appropriate, the controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of processing operations.

10. Where processing pursuant to point (c) or (e) of Article 6(1) has a legal basis in Union law or in the law of the Member State to which the controller is subject, that law regulates the specific processing operation or set of operations in question, and a data protection impact assessment has already been carried out as part of a general impact assessment in the context of the adoption of that legal basis, paragraphs 1 to 7 shall not apply unless Member States deem it to be necessary to carry out such an assessment prior to processing activities.

11. Where necessary, the controller shall carry out a review to assess if processing is performed in accordance with the data protection impact assessment at least when there is a change of the risk represented by processing operations.

Recitals 89 to 96:

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

Art 35 GDPR is closely linked to Art 24, 25, and 32. The main difference between Art 32 and Art 35 is that Art 32 (Security of data processing) is targeting risks linked to detrimental events such as attacks, while a Data Protection Impact Assessment (DPIA) based on Art 35 **is focusing primarily on risks, emerging from regular data processing.**

DPIA is an important tool for the implementation of data protection by technological means (data protection by design) as laid down in Art 25, Sec 1. Both are based on the principle of precaution, i.e. to identify risks already in the early design phases to consider relevant countermeasures before any data processing systems are implemented and become operational.

DPIA is a tool to identify and analyse such risks. In cases where a DPIA is not mandatory, an analysis of related risks is nonetheless required, to adequately implement Art 25 and Art 32. Both regulations explicitly refer to rights and freedoms of natural persons. The depth and required documentation of the risk analysis to be conducted depends on the complexity and the risk proneness of the processing. We recommend providing a documentation of the risk analysis in writing.

The implementation of the data protection by design principle reaches beyond the risks identified in advance in a state-of-the-art risk analysis and comprises decisions made at a later stage *ad hoc* by system developers (privacy engineering) when implementing the principle of data minimization.

2. When is a DPIA[1] required?

2.1. Basics

A DPIA has to be performed prior to processing of personal data carrying a high risk for rights and freedoms of natural persons.

In principle a DPIA has to be conducted for any form of data processing, unless it can be determined *a priori* that rights and freedoms of natural persons are not affected by a particular data processing operation.

For which type of data processing such a risk has to be assumed is e.g. laid down in points listed in Art 35, Para 3 or in recital 91? The emphasis here is on the use of so-

[1] The following text ist strongly based on the Publication in German Language of Kastelitz, M., Hötzendorfer, W., Riedl, R., Ausgewählte Fragen der Durchführung einer Datenschutz-Folgenabschätzung gemäß Art 35 DSGVO, Jahrbuch Datenschutzrecht 2017, 113ff.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

called new technologies, a vague legal concept, introduced in the GDPR with regard to DPIA. A risk assessment not only has to consider existing risk constellations, but also the probability of future events, to be identified in a prognostic assessment. The results of the assessment have to be documented.

Article 35 (1), last sentence, in conjunction with recital 92, provides an important point of view for assessing the need for a DPIA: "Under certain circumstances, it may be reasonable and economically appropriate not to apply a privacy impact assessment solely to a particular project but to broaden their thematic scope. For example, when public authorities or other public bodies want to create a joint application or processing platform, or when multiple stakeholders want to implement a joint application or processing environment for an entire business sector, market segment or widespread horizontal activity."

2.2. Cases where a DPIA is mandatory

Art 35 Sec 3 lists the mandatory cases for a DPIA:

(a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;
(b) processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10; or
(c) a systematic monitoring of a publicly accessible area on a large scale.

2.2.1. Further considerations regarding the need to conduct a DPIA

Recital 91 lists further cases requiring a DPIA:

Processing operations

(a) which potentially involve a large number of people, and/or a high level of risk and/or using a large-scale technology in line with the state-of-the-art;

b) which involve a high level of risk and make it difficult for data subjects to exercise their rights;

(c) where personal data are processed for taking decisions regarding specific natural persons following any systematic and extensive evaluation of personal aspects relating to natural persons based on profiling those data or following the processing of special

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

categories of personal data, biometric data, or data on criminal convictions and offences or related security measures;

(d) which involve a high level of risk because they prevent the persons concerned from exercising a right or use of a service or performance of a contract;

(e) which pose a high risk because they are systematically large scale.

2.2.2. Conducting a DPIA for several similar data processing systems

Art 35 Sec 1 states that a single DPIA can be performed for processing systems with similar risk level. When assessing such a similarity the overall purpose of the data processing in each individual case has to be considered. Recital 92 states that under consideration of economic costs DPIA can have a broader thematic scope, giving members in a specific industry sector or market segment the opportunity to cover applications or processing environments or widely shared horizontal practices with a single DPIA.

2.2.3. Positive and negative lists for DPIA

It can be assumed that regulatory agencies will publish positive/negative lists to guide the decision whether a DPIA is required in a specific case. These lists will define types of processing requiring a DPIA (“positive lists”) and cases where a DPIA is not required (“negative lists”). Both lists have to be forwarded by the national regulatory bodies to the European data protection board as part of the regime of regulatory coherence (Art 35 Sec 4) to provide for better harmonisation throughout the EU.

It has to be noted that Art 29 Working Party (WP29) recommends to conduct a DPIA also in cases, where it seems unclear whether a DPIA is required to help meeting the legal requirements for proper data protection.

2.3. Timing of DPIA

Timing and method applied for a DPIA have to be determined by the controller. Legal sanctions are foreseen for failing to perform a DPIA. It is recommended to start preparation for DPIA at the earliest possible stage of a project. Each department or relevant staff members involved in data processing have to initiate the relevant processes. Training is recommended to raise awareness about the need for DPIA within the organisation.

Considering measures for risk minimisation at an early stage of any project, involving data processing can help to keep bureaucratic efforts at a reasonably low level.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

A DPIA can guide the search for adequate solutions and can help to implement – as mentioned above – data protection requirements effectively and in due time through proper technological solutions (data protection by design) and the choice of default settings considering data protection.

Provided comprehensive and intensive preparations a DPIA will guide an envisaged project from the stage of early ideas to its final operational implementation and demonstrates the iterative nature of the DPIA process.

Whether a DPIA was required for processing activities that have been operative prior to the general applicability of GDPR (May 25, 2018) is an open question. Taking the literal wording ("prior to"), a DPIA is required only for processes becoming operative after May 25, 2018 or that undergo significant changes after this date.

Since in these cases the data processing system is already operative, a pre-check is not possible. Furthermore, these operations do not exist in an unregulated space (assuming all legal regulations and reporting requirements of the previous legal framework have been considered).

Nonetheless WP29 strongly recommends to perform DPIA for processing systems already in use to avoid legal uncertainties and even legal sanctions.

2.4. Review of the DPIA

After a DPIA has been performed the implementation of the measures suggested has to be reviewed, if deemed necessary a review of the data processing itself may be necessary to identify any new elements of the risks related to the processing of data. Recital 89 states that a review of the DPIA may be needed in due time after a first assessment. When conducting a DPIA, a time frame for routine checks or future renewals should be part of the documentation.

Technological developments, new legal regulation and changes in the processing routines have to be considered. Should a risk materialise, a new DPIA has to be performed.

The duty to perform a DPIA is part of the data controller's obligation, documenting their accountability. Documentation and report should not only provide information about the DPIA conducted, but also list any reasons for not preforming a full DPIA or for terminating a DPIA after having identified high risks for data subjects.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

2.5. Consultation with data protection authority pursuant Art 36 GDPR

The data controller has to consult with the Data Protection Authority (DPA) should the DPIA reveal major risks and should the controller not know how to take any remedial measures to mitigate such risks. The DPA has to respond to this request for consultation within fourteen weeks. For complex and innovative projects, it is recommended to start a DPIA at the earliest possible stage so any recommendation from the DPA can be considered in the implementation of the project plan.

3. Who is responsible to conduct a DPIA?

3.1. Basis

The responsibility of conducting a DPIA is with the controller – in this case the local public authority. Initially the Commission's proposal assigned responsibility for the DPIA to the data processor acting by the controller's order. In contrast, Recital 95 merely claims for the processor to assist the controller, where necessary and upon request, in ensuring compliance with the obligations deriving from the data protection impact assessment.

In practice, it will therefore be appropriate to contractually require a processor, if available and already selected, to the involvement and active support throughout the DPIA process. This is also beyond Article 28 (3) (f), which provides that the contract on the processing (or other legal instrument) should provide for the processor, taking into account the nature of the processing and the information at his/ her disposal, to ensure compliance with the obligations Articles 32 to 36. Often, only the processor will have the necessary information to assess the respective aspects of processing. In doing so, the risk of disclosure of trade and business secrets must be taken into account. Again, a corresponding contractual regulation is recommended. If processing of data by joint controllers is foreseen, the DPIA in the sense of Art. 35, para. 1, subpara. 2 may also be carried out by one of the controllers – which does not release other controllers of the responsibilities.

3.2. Participation in the DPIA

The DPIA should be organised as a project and as such should be equipped with the necessary material and human resources by a corresponding high level of management. When compiling the project team, particular attention must be paid to the complexity of the project, the required specialist knowledge and the required knowledge about the specific project and its environment. In practice, a team of lawyers, IT staff, CISO, data protection officer, the department that has requested processing ("data owner"), etc. can be put together.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

Particular attention is paid to ensuring the avoidance of conflicts of interest. Thus, those who deal with data processing in the future are not to be considered as independent, but on the other hand can provide valuable input to the design of the privacy impact assessment. Implementation can be done by an internal team as well as by external third parties. Ideally, an independent body should be involved.

The controller must seek the advice of the Data Protection Officer. Pursuant to Article 39 (1) (c), advice on the DPIA and the monitoring of its implementation are among the statutory duties of the DPO, but only on request and not in a leading position.

Therefore, there is an obligation on the controller to obtain the advice of the Data Protection Officer. At what time and to which degree the data protection officer needs to be involved in the process is the controller's decision. A subsequent review of the final report would also be sufficient. In practice, the timely involvement of the data protection officer, not least due to his expertise, is strongly recommended.

Depending on the organization of the controller, it is advisable to have the DPIA approved on management level or the corresponding authorised body.

4. How to conduct a DPIA

4.1. Basis

It has to be pointed out that the GDPR does not prescribe any specific form or concrete method of designing a data protection impact assessment which is currently being intensively discussed at national and European level. WP29 states that different design options can be used to support the implementation of the provisions of the GDPR and refers to examples of existing (generic or sector-specific) DPIA process models in Annex 1.[2]

4.2. Implementation of a DPIA

The controller is therefore basically free in how to carry out the DPIA process and can adapt it to the existing internal procedures, provided that the local public authority takes into account the four requirements contained in Article 35 (7) of the GDPR (a) to (d) as minimum requirements of a DPIA, which the Article 29 Working Party describes in more

2 WP29, WP 248, 15: Different methodologies (see Annex 1 of WP248 for examples of data protection and privacy impact assessment methodologies) could be used to assist in the implementation of the basic requirements set out in the GDPR (Annex 1).

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

detail and takes into account additionally the point "interested parties are involved" (see Art 35 para 2) and the view of the data subjects [see Art 35 para 9]):

(a) a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;

(b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes;

(c) an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1; and

(d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.

4.3. Minimum content of a DPIA

Article 35 (7) (a) to (d) GDPR in conjunction with recitals 84 and 90 thus requires as minimum:

1. a systematic description of the whole subject of evaluation ("target of evaluation"; embedded in the context, not just the pure data processing) and the purpose of the processing,

2. an evaluation of proportionality; also described in the literature as a normative evaluation of the planned data processing regarding its necessity and proportionality with regard to the purpose intended for it, in the sense of a purpose-means relation (beyond its mere admissibility),

3. a risk assessment, which consists of the three steps:

3.1 risk identification,

3.2 risk analysis (qualitative categorization according to the severity of the risk and its probability of occurrence),

3.3 risk assessment (for example by means of a risk matrix); and

4. risk treatment (taking risk management measures)

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

Points 3 and 4 are manifestations of the GDPR's so-called "risk-based approach", which are relevant not only in the implementation of a DPIA but also in the context of Articles 24, 25 and 32 GDPR. In other words, the DPIA is a specific example of the risk-based approach to data processing, for data, in short, that is expected to entail a high risk to the rights and freedoms of natural persons and calls for more extensive risk assessment and treatment. In principle, however, any other admissibility check on data processing is also inherent in such a risk assessment, including adequate technical and organisational measures that minimize risk, before they are implemented (see only Art. 24 (1) GDPR).

4.4. The DPIA Process

The DPIA should be seen as a process (not just a report) that should be started as soon as possible to influence the design of the subject ("project"). As a result, an impact assessment also differs from an audit that evaluates a project ex-post and usually comes too late to "buffer" the data protection needs that DPIA should produce.

There are now numerous proposals for the implementation of a DPIA process, which in one way or another are similar to the results of the PIAF study (2012)[3], which mapped the Privacy Impact Assessment methodologies in seven countries (including Derivation of "Best Practice" recommendations and core elements of a Privacy Impact Assessment process) for the EU Commission, among others. The following core elements were identified:

1. Determining whether a PIA is necessary (threshold analysis).
2. Identifying the PIA team and setting terms of reference.
3. Description of the proposed project [and identification of stakeholders].
4. Analysis of the information flows and other privacy impacts.
5. Consultation with stakeholders.
6. Risks management [Identification of risks and possible solutions].
7. Legal compliance check.
8. Formulation of recommendations.
9. Preparation and publication of the report [e.g., on the organisation's website].
10. Implementation of recommendations.
11. External [Third-party] review and/or audit.
12. Revisiting PIA if the project in question changes [Updating the PIA if there are changes in the project].

[3] *De Hert/Kloza/Wright* (Hrsg), PIAF, Recommendations for a privacy impact assessment framework for the European Union, Deliverable D3 (2012), http://piafproject.eu/ref/PIAF_D3_final.pdf; more available at http://piafproject.eu/Deliverables.html.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

The DPIA model for smart grids and smart metering systems, which is explicitly referred to in Recommendation 2014/724/EU of the European Commission, provides for the following steps:[4]

1. Step 1 Pre-assessment and criteria determining the need to conduct a DPIA.
2. Step 2 Initiation.
3. Step 3 Identification, characterisation and description of smart grid systems / applications processing personal data.
4. Step 4 Identification of relevant risks.
5. Step 5 Data protection risk assessment.
6. Step 6 Identification and recommendation of controls and residual risks.
7. Step 7 Documentation and drafting of the DPIA Report.
8. Step 8 Review and maintenance.

The new ISO / IEC 29134 standard provides guidelines for a process for conducting Privacy Impact Assessments and for the structure and content of a PIA report. The process is divided into the following four sub-processes:

1. Threshold analysis.
2. Preparation of the PIA.
3. Perform the PIA.
4. Follow-up of the PIA.

In which and how many sections a DPIA process is divided is rather a matter of taste, further suggestions range for example from three or four phases over six to seven stages. Rather, what is important is the comprehensible structure and process of the process, which in particular takes into account the requirements of Art. 35 (7) GDPR and the recommendations of the Article 29 Working Party.

4.5. Inclusion of data subjects or their representatives

Pursuant to Article 35 (9), where appropriate, the controller shall seek the views of the data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interest or the safety of the processing operations. The inclusion of the word "where appropriate" in the context of the trialogue negotiations makes it unclear under what circumstances the position of the person concerned or their

4 Commission Recommendation 2014/724/EU of 10 October 2014 on the Data Protection Impact Assessment Template for Smart Grid and Smart Metering Systems, ABl L 2014/300, 63.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

representative should be obtained in concrete terms and in which cases (permissible) this can be waived.

The way in which the opinion is requested is context-sensitive and the WP29 recognises different ways of doing so, such as conducting a study (internal or external), formal interviews with staff representatives or trade unions and submitting a questionnaire to future customers of the controller. The controller will have to deal with the views of the data subjects or their representatives and will have to address them in the impact assessment. Whether consumer protection associations can also be subsumed under the term "representative" is controversial in the literature.[5]

In any event, the obligation to consult *expressis verbis* is without prejudice to the protection of commercial or public interests or the safety of processing operations. Therefore, the controller may restrict or refuse in extremis the obligation to provide information on the intended processing under Article 35 (9) to the persons or representatives concerned (which, in the latter case, will lead to the fact that *a priori* involvement in the sense of Article 35 (9) will not be possible, since the existence of sufficient information is a *sine qua non* for the opinion of the persons concerned or their representatives).

For the implementation of the Data Protection Impact Assessment, it is recommended to document in the report for evidence purposes why no or only a limited content point of view has been obtained or the opinion obtained has not or only partially been taken into account.

4.6. The report on the implementation of a data protection impact assessment

It should be noted at this point that the DPIA report is not the actual goal of a DPIA, but a "means to an end" to document the process (internal and external). The reporting should not be underestimated – it documents the implementation and the results, and a mere "PR DPIA report" is to be avoided for reasons of compliance. The report can also serve as a guide and checklist in the conduct of the DPIA.

Art. 35 GDPR contains, somewhat surprisingly, no explicit requirement to prepare a report on the conduct of a DPIA. However, the fact that there is a duty of documentation for the

5 *Martini* in Paal/Pauly (Hrsg), Datenschutz-Grundverordnung (2016) Art 35 Rz 60; dagegen (mangels rechtlicher Verbundenheit) *Laue/Nink/Kremer*, Das neue Datenschutzrecht in der betrieblichen Praxis (2016) 245 Rz 99.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

controller is undoubted and follows implicitly from Article 35 (7) GDPR, and also from Article 5 (2) GDPR (accountability) in conjunction with Article 24 (1) GDPR and Article 36 (3) (e) (which requires the controller to provide "the data protection impact assessment referred to in Article 35"). Also, the review required by Article 35 (11) to assess whether processing is carried out in accordance with the DPIA requires that the results of the impact assessment be maintained. In addition, reporting on DPIAs carried out is in line with global good practice in this area (see section IV.1 below), which is evidently based on the DPIA provided for in Art. 35 GDPR.

Accompanying the DPIA process with documentation in the sense of a "living document" is recommended, beginning with the documentation of the threshold value analysis, in case of no necessity of carrying out a DPIA has been found. Even if this analysis shows that a DPIA is not required and the process is aborted, the controller will be responsible for its accountability and evidence. This written documentation may be submitted to the supervisor in any future process and will track internal considerations and assessments.

In terms of content, the DPIA report essentially sets out the procedure (including presentation of the facts in the sense of a systematic description of the entire subject of the test - "target of evaluation") and the results of the DPIA process. As in the case of the DPIA process itself, the GDPR does not provide for any specific rules for the design of a DPIA report. However, as minimum content, the criteria listed by the Article 29 Data Protection Working Party in Annex 2 of WP 248, which are essentially based on Article 35 (7), are predetermined. ISO / IEC 29134 recommends the following contents of the report on a Privacy Impact Assessment, with a focus on risk assessment:

1. Relevant privacy requirements.
2. Description of the scope.
3. Description of the risk criteria used.
4. Participants in the implementation.
5. Consulted stakeholders.

This is also supported by Recital 90, which states, inter alia, as follows: "*[t]hat impact assessment should include, in particular, the measures, safeguards and mechanisms envisaged for mitigating that risk, ensuring the protection of personal data and demonstrating compliance with this Regulation*"

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

In the very detailed PIAF study, the minimum content of a PIA report is as follows: [6]

1. Introduction and background information including who undertook the PIA, her contact details and where to find further information and other sources of help and advice.
2. A description of the project, of the information flows and of the impacts on privacy.
3. Results of the consultation of stakeholders.
4. Description of the risk assessment and risk mitigation phases, including the alternatives considered.
5. Analysis of legal compliance.
6. Recommendations.
7. Annexes, if necessary.

If the report or a final draft is available, the question may arise as to what has to happen to the person responsible (internally), above all whether and by whom this is to be "approved" - a practically relevant point which remains unmentioned in the GDPR. The ICO explicitly stipulates the following in its Code of Practice: "[o]btain appropriate signoff within the organisation". Since the person responsible has to carry out the DPIA, it follows that appropriately authorized representatives of the responsible person are involved in the DPIA and also have the ultimate responsibility. The management level will usually have final decision-making authority over the subject and nature of the DPIA project. As a minimum variant, the project management or data protection officer should report to the "highest management level", as provided for in Art. 38 (3) GDPR.

The GDPR has no obligation to publish the DPIA, but WP29 recommends its publication (at least in part) in order to increase confidence in data processing and to promote transparency. In particular, publication is encouraged in cases where part of the public will be affected by the (planned) processing.

5. Conclusions and practical tips

In particular, well-resourced regulatory agencies have developed their own approaches to privacy impact assessment over the years. From today's perspective, it is to be expected that those data protection authorities which have already developed their own model will prefer or propagate this, not least because the knowledge of the respective supervisory authority about their own recommendations will be most pronounced. The

6 *De Hert/Kloza/Wright* (Hrsg), PIAF, Recommendations for a privacy impact assessment framework for the European Union, Deliverable D3 (2012) 31, http://piafproject.eu/ref/PIAF_D3_final.pdf.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

contents of the currently available models of national supervisory authorities (from EU member states) are often prior to the GDPR and are not (yet) consistently adapted to the requirements or the terminology of the GDPR.

However, the ICO added its PIA Code of Practice (2014) to the (worth reading) report on "Big data, artificial intelligence, machine learning and data protection"[7] to the requirements and terminology of the GDPR, which is expected of other data protection authorities. It also remains to be seen whether the European Data Protection Board (Art. 68) will provide guidelines, recommendations and / or best practices for DPIA in accordance with Art. 70 (1) (e).

Recommendations at a glance:

- Documentation of all decisions, in particular why no DPIA has been carried out (if applicable);
- If in doubt, carry out a DPIA:
- Involvement of internal and external stakeholders;
- Using patterns, best practices, and, if appropriate, similar DPIAs already in place
- Publishing the DPIA:
  - Especially by public authorities;
  - Increases privacy awareness and builds trust;

6. External Sources & WEBLINKS

6.1. Books and Articles

- ***Kastelitz, M., Hötzendorfer, W., Riedl, R***., Ausgewählte Fragen der Durchführung einer Datenschutz-Folgenabschätzung gemäß Art 35 DSGVO, Jahrbuch Datenschutzrecht 2017, 113ff.
- ***De Hert, Paul/Kloza, Dariusz/Wright, David,*** Recommendations for a privacy impact assessment framework for the European Union http://www.piafproject.eu/ref/PIAF_D3_final.pdf
- ***Wright, David/De Hert, Paul* (Ed.),** Privacy Impact Assessment, Springer Science & Business Media, Dordrecht, Heidelberg, London, New York 2012
- ***De Hert/Kloza/Wright*** (Ed.), **PIAF**, Recommendations for a privacy impact assessment framework for the European Union, Deliverable D3 (2012),

[7] ICO, Big data, artificial intelligence, machine learning and data protection (2017), 99 f, https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

http://piafproject.eu/ref/PIAF_D3_final.pdf; more available at http://piafproject.eu/Deliverables.html.

- ***Martini in Paal/Pauly*** (Ed.), Datenschutz-Grundverordnung (2016) Art 35 Rz 60; dagegen (mangels rechtlicher Verbundenheit) Laue/Nink/Kremer, Das neue Datenschutzrecht in der betrieblichen Praxis (2016) 245 Rz 99.

6.2. Documents of the Article 29 Working Party

- Artikel-29-Working Party, WP 248, April 4, 2017: Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679 http://ec.europa.eu/newsroom/document.cfm?doc_id=44137
- WP 248, as last Revised and adopted on 4 October 2017 (rev.01): Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679 https://www.dsb.gv.at/documents/22758/112500/Guidelines_on_Data_Protection_Impact_Assessment_(DPIA).pdf/ed5daa8c-d388-43a6-9842-629b8175a99c

6.3. Web Links

- Brussels Laboratory for Data Protection and Privacy Impact Assessments http://www.vub.ac.be/LSTS/dpialab/
- ICO, Big data, artificial intelligence, machine learning and data protection (2017), 99 f, https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

ProLegis

Transparency

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

ProLegis

Contents

1. LEGAL FRAMEWORK 4
   1.1. Treaties of the European Union 4
   1.2. Charter of Fundamental Rights of the EU 4
   1.3. GDPR 4
2. THE MEANING OF TRANSPARENCY UNDER GDPR 5
   2.1. Elements of transparency under GDPR (Art. 12) 6
      2.1.1. "Concise, transparent, intelligible and easily accessible" 6
      2.1.2. "Clear and plain language" 6
      2.1.3. Manner of provision of information (art. 12, para 1 & para 5 "free of charge"). 6
   2.2. Information to be provided to the data subjects (Art. 13 & Art. 14) 7
      2.2.1. What information should be provided? 7
      2.2.3 How the information should be provided? 8
      2.2.4. When to provide information? 9
      2.2.5. When to provide notification in case of changes to the transparency information data controllers should provide? 9
   2.3. Modalities 9
      2.3.1. Privacy notices/ statements 9
      2.3.2. "Push" & "pull" notices 9
      2.3.3. Other types of "Appropriate measures" 10
      2.3.4. Visualisation 10
   2.4. Exercise of data subject rights 10
      2.4.1.Exemptions of the obligation to provide information 11
3. CONCLUSION & PRACTICAL ADVICES 11
4. EXTERNAL SOURCES & WEBLINKS 13

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

Books 13
Documents of the Article 29 Working Party 13
Web Links 13
5. REFERENCES 13

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

1. LEGAL FRAMEWORK

1.1. Treaties of the European Union

Article 1 of the TEU -> decisions being taken "as openly as possible and as close to the citizen as possible";

Article 11(2) TEU -> "The institutions shall maintain an open, transparent and regular dialogue with representative associations and civil society";

Article 15 of the TFEU -> citizens of the Union having a right of access to documents of Union institutions, bodies, offices and agencies and the requirements of those Union institutions, bodies, offices and agencies to ensure that their proceedings are transparent.

1.2. Charter of Fundamental Rights of the EU

Transparency is a vital element of the principle to fair processing. As such transparency is encompassed by Article 8 of the Charter of Fundamental Rights of the EU.

Article 8

Protection of personal data

1. Everyone has the right to the protection of personal data concerning him or her.

*2. Such data must be processed **fairly** for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.*

3. Compliance with these rules shall be subject to control by an independent authority.

1.3. GDPR

Recital 39

It should be transparent to natural persons that personal data concerning them are collected, used, consulted or otherwise processed and to what extent the personal data are or will be processed. The principle of transparency requires that any information and communication relating to the processing of those personal data be easily accessible and easy to understand, and that clear and plain language be used. That principle concerns, in particular, information to the data subjects on the identity

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

of the controller and the purposes of the processing and further information to ensure fair and transparent processing in respect of the natural persons concerned and their right to obtain confirmation and communication of personal data concerning them which are being processed…

Recital 58

The principle of transparency requires that any information addressed to the public or to the data subject be concise, easily accessible and easy to understand, and that clear and plain language and, additionally, where appropriate, visualisation be used. Such information could be provided in electronic form, for example, when addressed to the public, through a website. This is of particular relevance in situations where the proliferation of actors and the technological complexity of practice make it difficult for the data subject to know and understand whether, by whom and for what purpose personal data relating to him or her are being collected, such as in the case of online advertising. Given that children merit specific protection, any information and communication, where processing is addressed to a child, should be in such a clear and plain language that the child can easily understand.

Article 5, para 1

Principles relating to processing of personal data

1. Personal data shall be:

(a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');

2. THE MEANING OF TRANSPARENCY UNDER GDPR

The principle of transparency is linked to the principles of fairness and accountability. Article 5 (Principles relating to processing of personal data) obliges the controllers to demonstrate that personal data are processed in a transparent manner. According to the Article 29 Data Protection Working Party[i], transparency is aimed at empowering data subjects to hold data controllers and processors accountable and to exercise control over their personal data[ii]. This objective is realised by introducing specific practical requirements, which should be complied with on all stages of processing: before or at the start of the data processing when the personal data is being collected and throughout the whole processing period.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

2.1. Elements of transparency under GDPR (Art. 12)

2.1.1. "Concise, transparent, intelligible and easily accessible"

The first two parts of this requirement mean that data controllers should present the information/ communication efficiently and in a brief manner to avoid information fatigue (or otherwise said to overwhelm the data subjects with information). A way to do so may be layered notices, where subjects are informed of their rights on step by step basis (for example providing the key information in a short notice and the rest – at the point of collection of the data). This information should be separate from other non-privacy related information, such as contractual provisions.

The requirement that information is "intelligible" means that it should be understood by an average member of the intended audience, in the current case, by the average citizen of the local community. Data subjects should be able to determine in advance what the scope and consequences of the processing are. The Art. 29 Working Party (WP29) advices that data controllers spell out in unambiguous language what the most important consequences of the processing will be, especially if such consequences may have impact on the fundamental rights of the subjects[iii].

The "easily accessible" element means that the data subject should not have to seek out the information. Instead, it should be presented in an obvious manner, so the subject can access it without effort.

2.1.2. "Clear and plain language"

The requirement for clear and plain language means that information should be provided in as simple a manner as possible, avoiding complex sentence and language structures. The information should not be phrased in abstract or ambivalent terms or leave room for different interpretations[iv]. The purposes and legal basis for processing of personal data should be clear. Any unclear formulation of the purposes of processing such as "for development of future services" of "for research purposes" must be avoided. The information provided to a data subject should not contain overly legalistic, technical or specialist language or terminology[v].

Local authorities should also ensure that the vocabulary, tone and style of the language used when addressing children is appropriate to and resonates with children so that they recognise that the message/ information is being directed at them[vi].

2.1.3. Manner of provision of information (art. 12, para 1 & para 5 "free of charge").

Data controllers cannot charge data subjects for the provision of information under Articles 13 and 14 (information to be provided to the data subject), or for communications and actions taken under Articles 15 - 22 (rights of data subjects) and Article 34

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

(communication of personal data breaches to data subjects). There is one exception from this rule: when requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character. In this case, the controller may charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested. It is important for data controllers to know that they bear the burden of demonstrating the manifestly unfounded or excessive character of the request. Therefore, it is not advisable to local authorities to charge for the provision of information under GDPR to citizens.

2.2. Information to be provided to the data subjects (Art. 13 & Art. 14)

2.2.1. What information should be provided?

Articles 13 and 14 of GDPR stipulate what information must be provided to the data subject. The Regulation distinguishes cases when the information was provided by the subject (Art. 13) from cases when it was not (Art. 14). Local authorities should provide:

1) information about their identity, including their contact information;
2) contact details of the Data Protection Officer;
3) purposes of processing and their foundation in law – mostly for local authorities the foundation would be Art.6, para 1, lit. d), exercise of official authority vested in the controller, and the respective provisions of the legislation of the Member State;
4) the type of data that is processed, when it was not provided by the data subject;
5) the identity of the possible recipients of the data – this does not only include third parties, but also processors and joint controllers. The controller should be as specific as possible when defining the different categories of data recipients.

2.2.2 What additional information should be provided?

First, to ensure fair and transparent processing, the controller must provide the data subject with:

1) the period for which the personal data will be stored, or the criteria used to determine that period;
2) the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability;
3) where the processing is based on consent, the existence of the right to withdraw consent at any time;
4) the right to lodge a complaint with a supervisory authority;
5) the existence of automated decision-making, including profiling, and meaningful information about the logic involved, as well as the significance and the envisaged

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

consequences of such processing for the data subject.

The information about the profiling should not only be easily accessible for data subjects, but it must be brought to their attention. The controller should find simple ways to tell the data subject about the logic or the criteria used for the automated decision-making without complex explanations of the algorithms.

When the data was not obtained from the data subject, the data controller should provide her or his source. If the data subject provides the data, the controller should inform him of her if the provision of personal data is a statutory requirement.

Second, controllers should inform the data subjects if they plan to process the data for any purposes, different than the ones for which the data was collected. Data subjects must be provided with information on that other purpose and with any relevant further information, identical to the information provided for the initial purpose (period for processing, legal basis for processing, etc). When obtaining data, it could be useful to inform data subjects for eventual future processing, if it is likely it will be conducted given the activity of the controller.

2.2.3 How the information should be provided?

The default way of providing information to and communicating with data subjects is in writing. However, the GDPR also permits information to be provided by other means, including electronic. According to the WP29, it is critical that the methods chosen to provide the information are appropriate to the particular circumstances[vii]. Information may be provided orally to a data subject on request, if their identity information is proven by other (i.e. non-oral) means. There is an exception from this rule, concerning the information data controllers should provide under Art. 13 and 14 – this information could be disclosed to the subject without identity check. The oral provision of information does not necessarily mean oral information provided on a person-to-person basis, it could also mean automated oral information. According to the WP29, the data controller should allow the data subject to re-listen to pre-recorded messages, especially when it concerns visually impaired data subjects or other data subjects who may have difficulty in accessing or understanding information in written format. Also, in cases of oral provision of information, data controllers should still be able to demonstrate that they complied with the GDPR's requirements. In order to do so, they should ensure that they have a record of 1) the request for the information by oral means, 2) the method by which the data subject's identity was verified and 3) the fact that information was provided to the data subject[viii].

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

2.2.4. When to provide information?

Information about the processing of personal data should be given to the data subject at the time of the collection from it (Art. 13, Para 1). Where data is not directly obtained from the data subject but from another source, the information shall be provided to the data subject within a reasonable period, but at latest within 1 month from the obtainment, depending on the circumstances of the case. There are two specific cases: first, when the data is used for communication with the subject, the information should be provided at the latest at the time of the first communication to that data subject; and second, if is expected that the data will be disclosed to another recipient, at the latest at the first disclosure to that recipient.

2.2.5. When to provide notification in case of changes to the transparency information data controllers should provide?

In situations where the change to the information may have serious impact on the data subject, data controllers should provide information well in advance of the change actually taking effect[ix]. This should be done in an explicit and effective manner. Citizens should have enough time to consider the nature and impact of the change and exercise their rights under the GDPR in relation to the change, for example to object to the processing. The WP29 recommends reminding data subjects of the scope of data processing on a regular basis[x].

When planning to process the data for a different purpose than the ones it was obtained for, data subjects should be informed before the new processing has started.

2.3. Modalities

Modalities are the formats in which data controllers fulfil their obligation under the GDPR to provide information to the data subjects.

2.3.1. Privacy notices/ statements

Regarding online platforms, the use of an approach of layered privacy statements/ notices to link to the various categories of information which must be provided to the data subject, instead of using a single notice[xi]. This approach allows users to navigate directly to the section of the notice that they wish to read. When constructing such layered notice, controllers must aim to provide a clear and understandable overview (or content), so data subjects are aware where they can find each piece of information.

2.3.2. “Push” & “pull” notices

The Art. 29 Working Party also introduces the use of “push” and “pull” notices. The main difference is that in the latter case the users of a site are expected to request information, in particular the information on the processing of their data, while in the former case, the notice is “pushed” to their screen without any actions on their side. The WP29 gives

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union’s Rights, Equality and Citizenship Programme (2014-2020).

examples for push notices with “just-in-time” transparency information notices, and for “pull” notices – with transparency dashboards and “learn more” tutorials[xii]:

- *A just-in-time notice* is used to provide specific ‘privacy information’ when it is most relevant for the data subject to read. This format may be useful when a local authority’s website provides for a certain service to be performed online after filling a form. Before the citizen files the form, such just-in-time notice may appear.
- *Transparency dashboard* is a single point from which data subjects can view ‘privacy information’ and manage their privacy preferences by allowing or preventing their data from being used in certain ways.

2.3.3. Other types of “Appropriate measures”

Outside the digital environment, according to the WP29 appropriate measure may be:

- For hard copy/ paper environment: written explanations, leaflets;
- Telephonic environment: oral explanations by a real person, automated or pre-recorded information with options to hear more detailed information;
- QR codes, voice alerts, written information on the smart device, messages sent by SMS or email and others;
- Person to person environment: oral explanations, written explanations provided in hard or soft copy format[xiii].

2.3.4. Visualisation

The GDPR introduces visualisation tools (referencing in particular, icons, certification mechanisms, and data protection seals and marks). The idea of the icons is to convey the information to data subjects in an accessible way, using standardised symbols/images, recognised across the EU. The development of a “code of icons” has not yet started. The GDPR also provides for the use of data protection certification mechanisms, data protection seals and marks for the purpose of demonstrating compliance with the Regulation. Certification mechanisms are established by Member states, supervisory authorities, the European Data protection body or the Commission and are intended to demonstrate that the controller complies with the GDPR, showing that it is implementing technical and organisational measures to fulfil the standards for data protection. These formats may be applicable in entities which are not public authorities, such as an autonomous municipal company.

2.4. Exercise of data subject rights

Data subjects are entitled to receive information from the data controllers regarding their personal data. The information that must be provided under the GDPR is explicitly listed

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union’s Rights, Equality and Citizenship Programme (2014-2020).

in Art. 13 and Art. 14 and data subjects do not have to file a request or take any other active steps to acquire it, in contrast to when exercising their other rights (the right to access, rectification, erasure, etc.).

2.4.1.Exemptions of the obligation to provide information

The right to information is not absolute, or in other words, it is limited in certain situations. In certain cases, the local authorities are exempted from the obligation to provide the information outlined in Art. 13 & 14. When the data are acquired from the data subject, the only such case is when he or she already has the information (Art. 13, para 4).
When the data are not obtained from the subject, the exceptions are more (Art. 14, para 5):

- when the data subject already has the information;
- when the provision of such information proves to be impossible, would involve a disproportionate effort or would make the achievement of the objectives of the processing impossible or seriously impair them; an example of impossibility to provide information would be when the controller does not have any means to contact the data subject;
- when the obtaining or disclosure is expressly laid down by EU or EU Member State law, which would be the most common hypothesis for local authorities;
- when the personal data is subject to an obligation of professional secrecy regulated by Union or Member State law, including a statutory obligation of secrecy; this exception may be applicable to autonomous municipal companies and similar entities.

According to the WP29[xiv], these exceptions should, as a general rule, be interpreted and applied narrowly. The purpose of this recommendation is to limit the cases in which data controllers could apply the exceptions and to ensure higher protection of the rights of the data subjects.

3. CONCLUSION & PRACTICAL ADVICES

The principle of transparency is one of the foundations of the GDPR. It gives multiple guarantees that natural persons will have all the information they need in order to both be informed of what personal data is being processed about them and exercise their rights under the Regulation. The information should be easy to access and easy to understand with clear and plain language.
Local authorities are advised to make a list of all the information required by the GDPR and to choose the best modalities to reach the citizens, whose data they process. For

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

example, they can put up information posters in their public offices and distribute leaflets encompassing the information under Art.13 and Art. 14. The electronic means may be useful, for example if the entity has an online site/platform, but hard copy formats may also be necessary in certain cases. Special attention should be paid when local authorities' web portals offer online services. Also, it should be bore in mind that some autonomous municipal companies (such as public transport companies) execute numerous kinds of processing and deal with enormous data bases, therefore, they should put extra effort into composing the information under Art. 13 and 14 correctly.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

4. EXTERNAL SOURCES & WEBLINKS

Books

- **Voigt, P., von dem Bussche, A.**, The EU General Data Protection Regulation (GDPR) – A Practical Guide, Springer International Publishing (2017);
- Bird & Bird Guide to General Data Protection Regulation (2016);
- EU General Data Protection Regulation (GDPR). An Implementation and Compliance Guide, IT Governance Publishing, Cambridgeshire (2016);

Documents of the Article 29 Working Party

- Article 29 Data Protection Working Party, Guidelines on transparency under Regulation 2016/679, WP260;

Web Links

- http://europa.eu/rapid/press-release_IP-18-386_en.htm
- https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en

5. REFERENCES

[i] The Article 29 Working Party (WP) is established on the basis of Art. 29 of Directive 95/46/EC, which will be replaced by the GDPR. The goal of the WP is to provide opinions and recommendations and to advice on personal data protection.
[ii] Article 29 Data Protection Working Party, Guidelines on transparency under Regulation 2016/679, p. 23
[iii] Ibid, p. 8
[iv] Ibid, p. 9
[v] Ibid
[vi] Ibid
[vii] Ibid, p. 21
[viii] Ibid, p. 12
[ix] Ibid, p. 15
[x] Ibid, p. 16
[xi] Ibid, p. 17
[xii] Ibid, p. 17-18
[xiii] Ibid, p. 18-19
[xiv] Ibid, p. 25

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

ProLegis

Disclosure of information

or

Right of access by the data subject

Article 15 GDPR

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

Contents

1. Legal framework 3
   1.1. General Data Protection Regulation (GDPR) 3
2. Basics 5
3. Details of disclosing information to the data subject 5
   3.1. Substance of disclosure 5
   3.2. How much time has the controller to answer (deadline)? 6
   3.3. In what form can be claimed and how should it be answered? 7
   3.4. Has the applicant's identity as the data subject to be proven? 8
   3.5. Costs? May the information be reimbursed? 8
   3.6. Is there an obligation for the applicant to participate in the disclosure? 8
   3.7. Do the rights of third parties have to be taken into account when providing information? 9
4. Checklist for disclosing information on request 10
   4.1. Issuing the information 11
5. External Sources & WEBLINKS 12
   5.1. Books and Articles 12
   5.2. Other Documents and cases 12

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

1. Legal framework

1.1. General Data Protection Regulation (GDPR)

Article 15

Right of access by the data subject

1. The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:

(a) the purposes of the processing;

(b) the categories of personal data concerned;

(c) the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;

(d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;

(e) the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;

(f) the right to lodge a complaint with a supervisory authority;

(g) where the personal data are not collected from the data subject, any available information as to their source;

(h) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

2. Where personal data are transferred to a third country or to an international organisation, the data subject shall have the right to be informed of the appropriate safeguards pursuant to Article 46 relating to the transfer.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

3. The controller shall provide a copy of the personal data undergoing processing. For any further copies requested by the data subject, the controller may charge a reasonable fee based on administrative costs. Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form.

4. The right to obtain a copy referred to in paragraph 3 shall not adversely affect the rights and freedoms of others.

Recitals 63 and 64:

(63) A data subject should have the right of access to personal data which have been collected concerning him or her, and to exercise that right easily and at reasonable intervals, in order to be aware of, and verify, the lawfulness of the processing. This includes the right for data subjects to have access to data concerning their health, for example the data in their medical records containing information such as diagnoses, examination results, assessments by treating physicians and any treatment or interventions provided. Every data subject should therefore have the right to know and obtain communication in particular with regard to the purposes for which the personal data are processed, where possible the period for which the personal data are processed, the recipients of the personal data, the logic involved in any automatic personal data processing and, at least when based on profiling, the consequences of such processing. Where possible, the controller should be able to provide remote access to a secure system which would provide the data subject with direct access to his or her personal data. That right should not adversely affect the rights or freedoms of others, including trade secrets or intellectual property and in particular the copyright protecting the software. However, the result of those considerations should not be a refusal to provide all information to the data subject. Where the controller processes a large quantity of information concerning the data subject, the controller should be able to request that, before the information is delivered, the data subject specify the information or processing activities to which the request relates.

(64) The controller should use all reasonable measures to verify the identity of a data subject who requests access, in particular in the context of online services and online identifiers. A controller should not retain personal data for the sole purpose of being able to react to potential requests.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

2. Basics

The GDPR provides for in Article 15 the right to disclose all information available on the data subject upon on his or her request (e.g. customer, employee, job applicant, patient, hereinafter referred to as "data subject") vis-à-vis the controller (e.g. company, employer, hospital operator). This is called “Right of access of the data subject (to his or her data). The purpose of this right is that the data subject can obtain information about the content and the details of the data processed about him or her, with the aim of possibly asserting further data subject rights (e.g. a correction or deletion according to Art. 16 GDPR) or the lawfulness of the processing.

This right is a central institution of data protection law for it often has to be considered as the basis for the data subject to exercise any other rights. Although Data Protection Authorities (DPAs) under GDPR have the power to audit a controller without a particular complaint, in practise (due to limited resources of DPAs) it is typically an incomplete or late disclosure according to the data subjects right of access that calls the DPA on the plan. Thus, controllers should be well prepared for this process.

The best preparation however are well structured and best possible detailed records of processing activities. The better this documentation is shaped along the business processes for which personal data is processed, the easier one can find the particular data of a particular subject within the applications also in due time.

3. Details of disclosing information to the data subject

3.1. Substance of disclosure

The right of access entitles the data subject to the following:

i. The right to ask the controller to confirm whether or not his/ her personal data is being processed; if necessary, an inquiry should therefore be also answered “negative” if no data are processed about this person (so-called "negative information"): "We do not process data about you”;

ii. The right to obtain a copy of the personal data that is subject of the processing (for any additional copies requested by the data subject, the controller may charge a reasonable fee based on administrative costs.) If the data subject files the application electronically, then the information shall be provided in a common electronic format, unless otherwise stated.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

iii. The right to obtain following information:

Art 15 Para 1 GDPR	Content of the information
lit a	the **purpose of processing**
lit b	the c**ategories** of processed personal data
lit c	the **recipients or categories of recipients** to whom the personal data have been or could be disclosed, in particular recipients in third countries or international organisations
lit d	where possible, **the envisaged period for which the personal data will be stored**, or, if not possible, the criteria used to determine that period;
lit e	the **existence of the right to request from the controller rectification or erasure of personal data or restriction** of processing of personal data concerning the data subject or to object to such processing;
lit f	the **right to lodge a complaint** with a supervisory authority;
lit g	where the personal data are not collected from the data subject**, any available information as to their source**;
lit h	the existence of **automated decision-making**, **including profiling**, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.
Para 2	where personal data are **transferred to a third country or to an international organisation**, the data subject shall have the right to be informed of the appropriate safeguards pursuant to Article 46 relating to the transfer.

Note: According to Article 23, the **right to information could be restricted by national legislation**.

3.2. How much time has the controller to answer (deadline)?

In principle, the request for information must be answered promptly, but no later than within one month after receiving the application (Art. 12 (3) GDPR). This period may be extended for a further two months, if necessary, taking into account the complexity and the number of applications. The controller informs the data subject about the extension of the deadline within one month after receiving the request, together with the reasons for the delay. If the person concerned submits the application electronically, the data subject shall if possible be informed by electronic means, unless otherwise specified.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

If the controller does not act on the data subject's request, he/ she shall inform the data subject without delay, but no later than one month after receiving the request, of the reasons therefor and of the possibility to lodge a complaint with a supervisory authority or to lodge a judicial remedy.

3.3. In what form can be claimed and how should it be answered?

There is no compulsion to form, the request for information can be made orally, in writing or in digital form (for example by e-mail). The reply to a request for information may be made in any appropriate form, but the following should be noted:

- A written request is best answered in writing. One common method was in the past that the respondent submitted a copy of an identity document (official ID) to his/ her application and the person in charge gave the answer as registered mail (excluding delivery agents). However, as the official ID usually contains a larger amount of data necessary for the identification of the data subject, it is recommended that only information about the name, personal identification number, and/or the serial number of the ID document are submitted in writing by the data subject.
- If required by the applicant, the information may be provided orally provided that the identity of the data subject has been established in another form.
- If the data subject submits the application electronically (e.g. by e-mail), the information shall be provided in a common electronic format, unless otherwise specified. If possible, the controller may also provide remote access to a secure system that gives the data subject direct access to their personal information.

Attention! All communications must be conveyed **in a clear and simple language** in a precise, transparent, understandable and easily accessible form (this applies in particular to information that is aimed specifically at children). As in the past, the abbreviations contained in the answer have to be explained by the controller in his reply.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

3.4. Has the applicant's identity as the data subject to be proven?

Yes. The identity of the person requesting the information (the person concerned) must be clear, as the controller may request additional information if he has "reasonable doubt" about the identity of the natural person making the application (see Art. 12 para 6[1]).

According to recital 64, the controller should use all reasonable means to verify the identity of the data subject seeking information, in particular in the context of online services and in the case of online identifiers.

Identity authentication should be designed in order to fulfil the obligation to ensure data security in accordance with the risk, otherwise a data breach could occur if the data is transmitted to the wrong recipient.

A common practice in Austria under the previous Data Protection Act (DSG 2000) was that the applicant submitted a copy of an identification document (official ID) to his application and the controller gave the reply to the post office as a "personal" registered letter (excluding authorized agents). However, the identity may also be clear from the situation, e.g. if there is constant contact with the information provider and this (and its address) is therefore known[2].

3.5. Costs? May the information be reimbursed?

In principle, the information must be provided free of charge (see Art 12 para. 5 GDPR). However, in the case of manifestly unfounded or, in particular in the case of frequent repetition, excessive requests by a data subject, the controller may either:

(a) require a reasonable fee, taking into account the administrative costs of notifying or communicating or implementing the requested measure; or

b) refuse to act on the application.

3.6. Is there an obligation for the applicant to participate in the disclosure?

Yes, even if a duty to co-operate is mentioned only in Recital 63, in the literature published so far it is mainly assumed that it exists (such was also recognised in Austria under DSG 2000): "[w]here the controller processes a large quantity of information concerning the data subject, the controller should be able to request that, before the information is

[1] See also Souhrada-Kirchmayer, The right of access to the DSGVO, in Jahnel [Hrsg], Yearbook 17. Data Protection Law [2017] 86 f.

[2] See e.g. the jurisprudence of the Austrian High Courts: VwGH 4.7.2016, Ra 2016/04/0014; OGH 25.2.1993, 6 Ob 6/93)

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

delivered, the data subject specifies the information or processing activities to which the request relates."[3]

3.7. Do the rights of third parties have to be taken into account when providing information?

Yes, according to Article 15 (4) GDPR the right to receive a copy may not affect the rights and freedoms of others. In addition, Recital 63 further states *"[t]hat right should not adversely affect the rights or freedoms of others, including trade secrets or intellectual property and in particular the copyright protecting the software. However, the result of those considerations should not be a refusal to provide all information to the data subject."*

It is therefore necessary to control the data to be disclosed, as a rule, personal data of third parties (for example, the name of the person handling the customer and listed in the customer file) must be deleted from the data copy.

[3] Recital 63.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

4. Checklist for disclosing information on request

Am I obliged to provide information?	If the local public authority is a data controller – YES. If the local public authority is merely a processor, but still receives a request, it must immediately forward it to the person responsible.
Identity check	The identity of the person requesting the information (the person concerned) must be clear. If in doubt about the identity: Request proof
Is the disclosure of information free of charge?	In principle – YES. If the applicant was often given the same information or the request gravely troubles the controller, it is possible that a fee is envisaged. NB! This is a matter of national jurisdiction as well. Therefore, do check the applicable legislation on your activity.
Are there personal data of the applicant processed at all?	If no data has been stored about the applicant or if the data has already been deleted or the data has been irreversibly anonymised, no personal data will be processed, and a so-called negative information will be provided - "We do not process data about you".
What data and information does the controller have to provide?	All data must be provided that is stored from the person concerned. Depending on the complexity of the systems, it must be considered in advance (in terms of the processing directory) in which systems data of which category of affected persons can be found. In addition, the information listed in Article 15 (1) GDPR must be provided. Third party rights must be observed (esp. trade secrets and data of third parties are to be deleted / blackened).

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

4.1. Issuing the information

Example of a disclosure of information according to Article 15 GDPR

Your request for information

Dear Sir / Madam [name],

1. Your application from [date] to information pursuant to Art. 15 GDPR, received by us on [date], may be answered as follows:

2. [In the event of a response within the period of one month from receipt] We hereby confirm in time that we process personal data about you.

[in case of extension according to Art. 12 (3) GDPR] As stated in the letter of [date], we have taken the opportunity to extend the deadline to three months due to [complexity of the application or number of your requests, further explanation necessary].

3. [if no data is processed] No personal data will be processed. [Then continue with text module No. 9].

[When data is processed] Specifically, we process the following data about you: [here is a list of the actual data to be processed].

Printouts / copies from the relevant data processing can be found in the appendix. Any blackening or omission has been made so as not to affect the rights and freedoms of others, or because the information does not concern you or your personal information.

4. [if data was not collected from the data subject]: We have received your data from [available information on the origin of your data, e.g. public body XY].

5. [if applicable] We will use automated decision-making / profiling procedures that have a legal effect on you or similarly affect you in a similar way: [please complete meaningful information about the logic involved and the implications and implications].

6. You have the rights to rectification, deletion, restriction and the right to object processing of your personal data. For that, contact us. If you believe that the processing of your data violates data protection law or if your data protection claims have otherwise been violated in a way, you can complain to the supervisory authority. In this country, the XYZ is responsible.

Kind regards

….

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

5. External Sources & WEBLINKS

5.1. Books and Articles

- Souhrada-Kirchmayer, The right of access to the DSGVO, in Jahnel [Hrsg], Yearbook 17. Data Protection Law [2017] 86 f.
- ***Martini in Paal/Pauly*** (Ed.), Datenschutz-Grundverordnung (2016).

5.2. Other Documents and cases

- jurisprudence of the Austrian High Courts: VwGH 4.7.2016, Ra 2016/04/0014; OGH 25.2.1993, 6 Ob 6/93) Web Links
- To compare the changes to directive 95/46/EC see https://gdpr.report/news/2017/11/20/gdpr-subject-access-requests/

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

ProLegis

Правни основания за обработване на лични данни

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

Съдържание

1. ПРАВНА РАМКА 4

1.1. Харта на основните права на ЕС 4

1.2. Общ регламент за защита на данните (GDPR) 4

2. ПРАВНИ ОСНОВАНИЯ ЗА ОБРАБОТВАНЕ НА ЛИЧНИ ДАННИ ПО GDPR .. 11

2.1. Съгласие 11

2.1.1. Значение и правни изисквания 11

2.1.2. Приложимост по отношение на дейностите на местните власти 13

2.2. Изпълнение и сключване на договор с физическо лице 14

2.2.1. Значение и правни изисквания 14

2.2.2. Приложимост по отношение на дейностите на местните власти 15

2.3. Законово задължение 15

2.3.1. Значение и правни изисквания 15

2.3.2. Приложимост по отношение на дейностите на местните власти 17

2.4. Защита на жизненоважни интереси 17

2.4.1. Значение и правни изисквания 17

2.4.2. Приложимост по отношение на дейностите на местните власти 18

2.5. Изпълнение на задача от обществен интерес или при упражняването на официални правомощия 18

2.5.1. Значение и правни изисквания 18

2.5.2. Приложимост по отношение на дейностите на местните власти 19

2.6. Легитимни интереси 19

2.6.1. Значение и правни изисквания 19

2.6.2. Приложимост по отношение на дейностите на местните власти 20

3. ЗАКЛЮЧЕНИЕ И ПРАКТИЧЕСКИ СЪВЕТИ 21

4. ВЪНШНИ ИЗТОЧНИЦИ И ЛИНКОВЕ 21

Книги 21

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

Документи на работната група по чл. 29 21
Интернет линкове 21
5. ПРЕПРАТКИ 22

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

1. ПРАВНА РАМКА

1.1. Харта на основните права на ЕС

Член 8

Защита на личните данни

1. Всеки има право на защита на неговите лични данни.

2. Тези данни трябва да бъдат обработвани добросъвестно, за точно определени цели и въз основа на съгласието на заинтересованото лице или по силата на друго предвидено от закона легитимно основание. Всеки има право на достъп до събраните данни, отнасящи се до него, както и правото да изиска поправянето им.

3. Спазването на тези правила подлежи на контрол от независим орган.

1.2. Общ регламент за защита на данните (GDPR)

Съображение (42)

[…] За да бъде съгласието информирано, субектът на данни следва да знае поне самоличността на администратора и целите на обработването, за които са предназначени личните данни. Съгласието не следва да се разглежда като свободно дадено, ако субектът на данни няма истински и свободен избор и не е в състояние да откаже или да оттегли съгласието си, без това да доведе до вредни последици за него.

Съображение (43)

За да се гарантира, че е дадено свободно, съгласието не следва да представлява валидно правно основание за обработването на лични данни в конкретна ситуация, когато е налице очевидна неравнопоставеност между субекта на данните и администратора, по-специално когато администраторът е публичен орган, поради което изглежда малко вероятно съгласието да е дадено свободно при всички обстоятелства на конкретната ситуация. Смята се, че съгласието не е дадено свободно, ако не се предоставя възможност да бъде дадено отделно съгласие за различните операции по обработване на лични данни, макар и да е подходящо в конкретния случай, или ако изпълнението на даден договор, включително предоставянето на услуга, се поставя в зависимост от даването на съгласие, въпреки че това съгласие не е необходимо за изпълнението.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

Съображение (44)

Обработването на данни следва да е законосъобразно, когато то е ***необходимо в контекста на договор или при намерение за сключване на договор.***

Съображение (45)

Когато обработването се извършва в съответствие с правно задължение, наложено на администратора на лични данни, или когато обработването е необходимо за изпълнението на задача от обществен интерес или при упражняване на официални правомощия, за обработването следва да има основание в правото на Съюза или в правото на държава членка. Настоящият регламент не изисква за всяко отделно обработване конкретен законодателен акт. Може да е достатъчен законодателен акт като основание за няколко операции по обработване на данни, основаващи се на правно задължение, наложено на администратора на лични данни, или когато обработването е необходимо за изпълнението на задача от обществен интерес или при упражняване на официални правомощия. Правото на Съюза или на държава членка следва да определя също и целта на обработването. Нещо повече, в това право биха могли да се посочат общите условия на настоящия регламент, които определят законосъобразността на обработването на лични данни, да се установяват спецификациите за определянето на администратора на лични данни, видът данни, които подлежат на обработване, съответните субекти на лични данни, образуванията, пред които могат да бъдат разкривани лични данни, ограниченията по отношение на целите, периодът на съхранение и други мерки за гарантиране на законосъобразното и добросъвестно обработване. Също така в правото на Съюза или на държава членка следва да се определи дали администраторът на лични данни, изпълняващ задача от обществен интерес или упражняващ официални правомощия, следва да бъде публичен орган или друго физическо или юридическо лице, субект на публичното право или когато това е оправдано поради съображения от обществен интерес, включително за здравни цели, като например общественото здраве и социалната закрила и управлението на здравните служби субект на частното право, като например професионално сдружение.

Съображение (46)

Обработването на лични данни следва да се счита за законосъобразно и когато е необходимо, за да се защити интерес от първостепенно значение за живота на субекта на данните или на друго физическо лице. Обработването на лични

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

данни единствено въз основа на жизненоважен интерес на друго физическо лице следва да се състои по принцип, само когато обработването не може явно да се базира на друго правно основание. Някои видове обработване могат да обслужват както важни области от обществен интерес, така и жизненоважните интереси на субекта на данните, например когато обработването е необходимо за хуманитарни цели, включително за наблюдение на епидемии и тяхното разпространение или при спешни хуманитарни ситуации, по-специално в случай на природни или причинени от човека бедствия.

Съображение (47)

***Законните интереси на даден администратор, включително на администратор, пред когото може да бъдат разкрити лични данни, или на трета страна** могат да предоставят правно основание за обработването, при условие че интересите или основните права и свободи на съответния субект на данни нямат преимущество, като се вземат предвид основателните очаквания на субектите на данни въз основа на техните взаимоотношения с администратора. Такъв законен интерес може да е налице, когато например между субекта на данни и администратора на лични данни съществува съответното определено взаимоотношение, например когато субектът на данни е клиент или подчинен на администратора на лични данни. При всички случаи, за установяването на законен интерес би била необходима внимателна преценка, включително дали субектът на данни може по времето и в контекста на събирането на данни основателно да очаква, че може да се осъществи обработване на личните данни за тази цел. Интересите и основните права на субекта на данни биха могли по-конкретно да имат преимущество пред интереса на администратора, когато личните данни се обработват при обстоятелства, при които субектите на данни основателно не очакват по-нататъшна обработка. Като се има предвид, че е задължение на законодателя да уреди със закон правното основание за обработването на лични данни от публичните органи, това правно основание не следва да се прилага спрямо обработването на данни от публичните органи при изпълнението на техните задачи. Обработването на лични данни, строго необходимо за целите на предотвратяването на измами, също представлява законен интерес на съответния администратор на данни. Обработването на лични данни за целите на директния маркетинг може да се разглежда като осъществявано поради законен интерес.*

Съображение (48)

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

Администратори, които представляват част от група предприятия или институции, свързана с централен орган, могат да имат законен интерес да предадат личните данни в рамките на групата предприятия за вътрешни административни цели, включващи обработването на лични данни на клиенти или служители. Общите принципи на предаването на лични данни на предприятие, разположено в трета държава, в рамките на група предприятия, остават непроменени.

Съображение (49)

Обработването на лични данни в степен, която е строго необходима и пропорционална на целите на гарантирането на мрежовата и информационната сигурност, т.е. способността на дадена мрежа или информационна система да издържа, със съответно равнище на доверие, на случайни събития или неправомерни или злонамерени действия, които повлияват на наличността, автентичността, целостта и поверителността на съхраняваните или предаваните лични данни, както и на сигурността на свързаните услуги, предлагани или достъпни посредством тези мрежи и системи, от страна на публични органи, екипи за незабавно реагиране при компютърни инциденти (ЕНРКИ), екипи за реагиране при инциденти с компютърната сигурност (ЕРИКС), доставчици на мрежи и услуги за електронни съобщения и доставчици на технологии и услуги за сигурност, представлява законен интерес на съответния администратор на данни. Това може да включва например предотвратяването на непозволен достъп до електронни съобщителни мрежи и разпространение на зловреден софтуер и спиране на атаки с цел отказване на услугите и вреди за компютрите и електронните съобщителни системи.

Съображение (50)

Обработването на лични данни за цели, различни от тези, за които първоначално са събрани личните данни, следва да бъде разрешено единствено когато обработването е съвместимо с целите, за които първоначално са събрани личните данни. В такъв случай не се изисква отделно правно основание, различно от това, с което е било разрешено събирането на личните данни. Ако обработването е необходимо за изпълнението на задача от обществен интерес или свързана с упражняването на официални правомощия, които са предоставени на администратора на лични данни, в правото на Съюза или в

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

правото на държава членка могат да бъдат определени и уточнени задачите и целите, за които по-нататъшното обработване следва да се счита за съвместимо и законосъобразно. По-нататъшното обработване за целите на архивирането в обществен интерес,за целите на научни или исторически изследвания, или за статистически цели следва да се разглежда като съвместими законосъобразни операции по обработване. Правното основание, предвидено от правото на Съюза или правото на държава членка за обработване на лични данни, може да предостави и правно основание за по-нататъшно обработване. За да установи дали дадена цел на по-нататъшно обработване е съвместима с целта, за която първоначално са събрани личните данни, администраторът на лични данни, след като е спазил всички изисквания относно законосъобразността на първоначалното обработване, следва да отчете, inter alia,, всички връзки между тези цели и целите на предвиденото по-нататъшно обработване, в какъв контекст са събрани личните данни, по-специално основателните очаквания на субектите на данните въз основа на техните взаимоотношения с администратора по отношение на по-нататъшно използване на личните данни, естеството им, последствията от предвиденото по-нататъшно обработване на данни за субектите на данни и наличието на подходящи гаранции при операциите по първоначалното и предвиденото по-нататъшно обработване.

Член 4

Дефиниции

За целите на този Регламент:

[…]

(11) „съгласие на субекта на данните“ означава всяко ***свободно изразено, конкретно, информирано и недвусмислено указание за волята на субекта на данните, посредством изявление или ясно потвърждаващо действие, което изразява съгласието му свързаните с него лични данни да бъдат обработени.***

Член 6

Законосъобразност на обработването

1. Обработването е законосъобразно, само ако и доколкото е приложимо поне едно от следните условия:

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

а) субектът на данните е дал съгласие за обработване на личните му данни за една или повече конкретни цели;

б) обработването е необходимо за изпълнението на договор, по който субектът на данните е страна, или за предприемане на стъпки по искане на субекта на данните преди сключването на договор;

в) обработването е необходимо за спазването на законово задължение, което се прилага спрямо администратора;

г) обработването е необходимо, за да бъдат защитени жизненоважните интереси на субекта на данните или на друго физическо лице;

д) обработването е необходимо за изпълнението на задача от обществен интерес или при упражняването на официални правомощия, които са предоставени на администратора;

е) обработването е необходимо за целите на легитимните интереси на администратора или на трета страна, освен когато пред такива интереси преимущество имат интересите или основните права и свободи на субекта на данните, които изискват защита на личните данни, по-специално когато субектът на данните е дете.

Буква е) на първа алинея не се прилага за обработването, което се извършва от публични органи при изпълнението на техните задачи.

2. Държавите членки могат да запазят или въведат по-конкретни разпоредби, за да адаптират прилагането на правилата на настоящия регламент по отношение на обработването, необходимо за спазването на параграф 1, букви в) и д), като установят по-конкретно специални изисквания за обработването и други мерки, за да се гарантира законосъобразно и добросъвестно обработване, включително за други особени случаи на обработване на данни, предвидени в глава IX.

3. Основанието за обработването, посочено в параграф 1, букви в) и д), е установено от:

а) правото на Съюза или

б) правото на държавата членка, което се прилага спрямо администратора.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

Целта на обработването се определя в това правно основание или доколкото се отнася до обработването по параграф 1, буква д), то трябва да е необходимо за изпълнението на задача от обществен интерес или при упражняването на официални правомощия, които са предоставени на администратора. Това правно основание може да включва конкретни разпоредби за адаптиране на прилагането на разпоредбите на настоящия регламент, inter alia общите условия, които определят законосъобразността на обработването от администратора, видовете данни, които подлежат на обработване, съответните субекти на данни; образуванията, пред които могат да бъдат разкривани лични данни, и целите, за които се разкриват; ограниченията по отношение на целите на разкриването; периодът на съхранение и операциите и процедурите за обработване, включително мерки за гарантиране на законосъобразното и добросъвестно обработване, като тези за други конкретни случаи на обработване съгласно предвиденото в глава IX. Правото на Съюза или правото на държавата членка се съобразява с обществения интерес и е пропорционално на преследваната легитимна цел.

4. Когато обработването за други цели, различни от тези, за които първоначално са били събрани личните данни, не се извършва въз основа на съгласието на субекта на данните или на правото на Съюза или правото на държава членка, което представлява необходима и пропорционална мярка в едно демократично общество за гарантиране на целите по член 23, параграф 1, администраторът, за да се увери дали обработването за други цели е съвместимо с първоначалната цел, за която са били събрани личните данни, inter alia, взема под внимание:

а)всяка връзка между целите, за които са били събрани личните данни, и целите на предвиденото по-нататъшно обработване;

б)контекста, в който са били събрани личните данни, по-специално във връзка с отношенията между субекта на данните и администратора;

в)естеството на личните данни, по-специално дали се обработват специални категории лични данни съгласно член 9 или се обработват лични данни, отнасящи се до присъди и нарушения, съгласно член 10;

г)възможните последствия от предвиденото по-нататъшно обработване за субектите на данните;

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

д)наличието на подходящи гаранции, които могат да включват криптиране или псевдонимизация.

2. ПРАВНИ ОСНОВАНИЯ ЗА ОБРАБОТВАНЕ НА ЛИЧНИ ДАННИ ПО GDPR

2.1. Съгласие

2.1.1. Значение и правни изисквания

Съгласието е едно от шестте правни основания, изброени в чл. 6 на GDPR. За да бъде то валидно, GDPR изисква съгласието да бъде дадено свободно, конкретно, информирано и еднозначно.

- **‘свободно’** = предполага извършване на действителен избор и упражняване контрол от страна на физическите лица[i]. Ако настъпят някакви неблагоприятни последици за субекта на данни от това, че не е дал съгласието си/ оттеглил е вече даденото съгласие (например отказ на услуга, по-високи разходи за стока/ услуга – такси, цена и др.), съгласието не се смята за свободно дадено. Но тъй като в отношенията се местните власти и гражданите не са равнопоставени, съгласието рядко е подходящото правно основание за обработване на лични данни в контекста на упражняване на публични правомощия;
- **‘конкретно’** = това изискване е пряко свързано с изискването за съгласие на физическите лица с една или повече конкретни цели на обработването (т.нар. „разбивка“ на съгласието[ii]) и с принципа за конкретизиране на целта. Всяка от целите на обработването трябва да бъде ясно дефинирана за физическите лица от самото начало.
- субектът на данни трябва да има възможност да избере за кои цели на обработване да даде съгласие (например да се съгласи за целите А, Б и В, и да не се съгласи за целите Г и Д). Ако съгласието се събира в рамките на формуляр, информацията, отнасяща се до него, трябва да е ясно разграничена от информацията по други въпроси (пр. физически обособено в рамките на самия документ). Съгласието трябва да бъде взето за всяка нова цел на обработване и администраторите трябва с всяко искане за предоставяне на съгласие да предоставят конкретна информация за видовете данните, които се събират за всяка цел;

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

- **‘информирано’** = минималните изисквания по GDPR включват предоставяне на информация за администратора и за целите на обработването. Работната група по чл. 29 препоръчва включването на допълнителна информация като вида данни, които се събират и използват; правото да се оттегли съгласието; информация за използване на данните за решения, основани само на автоматично обработване, включително профилиране[iii]; при трансфери – информация за възможните рискове от трансфери на данни към трети страни в отсъствието на решение на Комисията относно адекватното ниво на защита и подходящи гаранции[iv].
- **‘еднозначно’** = съгласието трябва да се даде чрез изявление от физическото лице или ясен знак за потвърждение. Съгласието трябва винаги да се даде чрез активен жест или изявление. Следователно, мълчанието, предварително отбелязаните полета и бездействието не могат да се приемат за валидно съгласие по GDPR.
- **толкова лесно за оттегляне, колкото и за даване** = съгласие следва да може да се оттегли по всяко време. Това не е задължително да се случва със същото действие, но процесът по оттегляне трябва да е също толкова лесен, колкото и процесът по даване (например да се кликне на кутийка в онлайн декларация за съгласие да се получава вестника на общината е също толкова лесно, колкото да се кликне на линк в имейл към вестника, с който да се отпише и да се оттегли съгласието);
- **особени изисквания при събиране на съгласие от деца** = GDPR третира децата като уязвима категория физически лица. Следователно, те получават специална закрила, тъй като може да са по-малко наясно с рисковете, последиците и гаранциите, свързани с правата им по отношение на обработването на лични данни. При предоставяне на дете на услуги на информационното общество (например онлайн образователни кампании, проведени на сайта на общината, които изискват събиране на данни на децата), съгласие за обработването на данни на деца под 16 години (държавите членки могат да намалят тази възраст до 13 години) трябва да се получи от родителя или настойника.
- **съгласие по Директива 95/46** = съгласие**,** получено по стария режим, не е задължително да бъде събирано наново. Ако съгласието отговаря на изискванията на GDPR, то ще продължи да е валидно основание за обработване.

Администраторът на данни носи тежестта да докаже надлежното събиране на съгласие[v].

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

2.1.2. Приложимост по отношение на дейностите на местните власти

На практика съгласието рядко ще бъде основание за обработване на лични данни от местните власти. Това заключение може да се направи от изискванията, на които трябва да отговаря съгласието, за да е валидно.

Първо, фактът, че съгласието трябва да е „свободно дадено“, тоест че физическото лице не трябва да търпи никакви негативни последствия, ако не даде съгласието си, означава, че във всяка ситуация, в която местните власти са в ролята си на публична власт, съгласието не могат да бъде използвано като валидно правно основание. Контролът върху надлежното изпълнение на публичноправните задължения на гражданите (например събиране на местни такси, регистрация на недвижими имоти и МПС и други) и налагането на санкции в случай на неизпълнение на тези задължения са неизменно свързани с правото (и задължението) да се упражнява държавна принуда. Това означава, че физическите лица нямат истински свободен избор дали да се съгласят или не за обработването на личните им данни. Те са в подчинена роля и са задължени от закона да сътрудничат на местните власти.

Второ, съгласието може да бъде оттеглено „по всяко време“. Ако съгласието е правното основание за обработването на лични данни в случаи, когато гражданите изпълняват законовите си задължения, потенциално всеки недобросъвестен гражданин (например ако не иска да изпълнява определени публичноправни задължения) би могъл да оттегли съгласието си по всяко време и да използва това оттегляне да създава пречки за (и на практика да „блокира“) нормалното функциониране на местните власти. Ако съгласието се оттегли, местните власти като администратор трябва да прекратят обработването. Това е немислимо, когато се упражнява публични правомощия, защото би застрашило цялата идея за упражняване на публична власт. Следователно, в описаните ситуации съгласието не е правилният инструмент за подобно обработване.

Според Работната група по чл. 29, „използването на съгласието като правно основание за обработване от публични власти **не е напълно изключено** по GDPR” [vi]. Следователно, съгласието може да бъде полезен инструмент в ситуации, в които местните власти не изпълняват типичните си и основни функции или когато съответното обработване е незадължително (и има установени процедури по обработване, които се осъществяват когато лицето не даде съгласие). Примери са следните ситуации:

- местните власти и правителствени власти изискват една и съща информация за издаване на акт по искане на гражданина, но нямат достъп до базите данни на другите. Тъй като и двата вида власти изискват една и съща информация от гражданина, те биха могли да поискат съгласието на

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

гражданина да съединят файловете, за да избегнат двойни процедури и кореспонденция. И двата вида публични власти трябва да се уверят, че това не е задължително, и че издаването на документа ще бъде осигурено, дори и гражданинът да не се е съгласил за съединяването на данните[vii];

- местните власти предоставят опция да уведомяват граждани, участващи в административни процедури, по мейл. Режимът е да се заяви изрично желание (opt-in), тоест гражданите са свободни да решат дали да бъдат уведомени по мейл (например чрез отбелязване на кутийка в онлайн/ хартиен формуляр и предоставяне на електронен адрес). Обработването на електронния адрес в такъв случай ще се базира на съгласие;
- местните власти осигуряват на гражданите възможността да се запишат в бюлетин за получаване на покани за различни събития, организирани от местните власти (например изложби в местни музеи, театрални премиери в общински театър, кампании за събиране на боклук, състезания, образователни кампании, провеждани в общински училища). Записването изисква да се предоставят данни за контакт (например пощенски код, телефонен номер, имейл и т.н.), както и данни за предпочитанията на лицето (например хобита, интереси и т.н.). Обработването за такъв тип цели ще се основава на съгласие, тъй като гражданите могат да се отпишат за получаването подобни съобщения по всяко време, без негативни последствия.

2.2. Изпълнение и сключване на договор с физическо лице

2.2.1. Значение и правни изисквания

Разпоредбата на чл. 6, пар. 1, буква „б“ GDPR въвежда две самостоятелни правни основания за обработване:

(i) ситуации, в които обработването е необходимо за изпълнение на договор, по който физическото лице е страна;

(ii) ситуации, в които обработването се състои *преди* да се встъпи в договор. Това се отнася до преддоговорни отношения, стига стъпките към сключване на договор да са предприети по искане на лицето, а не по инициатива на администратора или на трето лице[viii].

Първата хипотеза трябва да се тълкува тясно и не би следвало да обхваща ситуации, в които обработването не е необходимо за изпълнението на договора, а е едностранно наложено на лицето от администратора[ix]. Според разбирането на Работната група по чл. 29 за същото основание по старата Директива 95/ 46, това правно основание се прилага само когато то е необходимо за **изпълнението** на договор. С други думи, стига обработването да попада в клаузите на нормалното

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

изпълнение на договора, то би могло да се базира на това правно основание. Това основание покрива всички ситуации, в които обработването се изпълнява в контекста на договор, независимо за коя фаза става дума[x]. Въпреки това, всички по-нататъшни действия, предизвикани от неизпълнение или от други проблеми при изпълнение (напр. забава), не подадат в обхвата на това правно основание. Подобни видове обработване ще изискват приложението на друго основание – например легитимните интереси на администратора, които имат преимущество.

Втората хипотеза включва обработване, необходимо за изготвяне на оферти, за дейности по набирането на служители и други. Въпреки това, всяка детайлна проверка на личното досие на кандидатите би била доста обширна и не би била обоснована като стъпки, изисквани от физическото лице.

Като цяло, това основание се тълкува стеснително от регулаторите, затова администраторите трябва да могат да демонстрират, че обработването е абсолютно необходимо за сключването на договора[xi].

2.2.2. Приложимост по отношение на дейностите на местните власти

Това правно основание за обработване на личните данни може да се приложи от местните власти най-малко в следните области:

- Обработване в контекста на трудови правоотношения – например обработване на информация за трудовото възнаграждение и информация за банкови сметки, за да може да се превежда възнаграждението[xii];
- Обработване в контекста на сключване на договори за обществени поръчки - това основание би могло да се препокрие с друго основание за обработване, а именно законовото задължение на местните власти в рамките на съответната административна процедура, наложено от местния закон.
- обработване в контекста на отношенията между частни организации, изцяло или частично притежавани от общината/държавата и гражданите – например от организации, предлагащи обществен транспорт в рамките на града/ общината, организации, предоставящи снабдителни услуги (електричество, газ, вода и др.) при изпълнението на съответните договори.

2.3. Законово задължение

2.3.1. Значение и правни изисквания

Това правно основание изисква наличие на ясна разпоредба на законово или на подзаконово равнище (така нареченото в някои държави вторично законодателство), която задължава администратора да осъществи обработването.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

Работната група по чл. 29 подчертава, че законът трябва да отговаря на всички условия, за да бъде задължението валидно и обвързващо, и трябва да съответства на законовите правила за защита на личните данни, включително изискванията за необходимост, пропорционалност и ограничение на целите[xiii]. GDPR изрично изисква това задължение да е едновременно:

(i) Задължение по закона на държавата членка или на ЕС, на което се подчинява администраторът. Работната група по чл. 29 вече е дала следното тълкувание по старата Директива 95/46 в това отношение: задължения по законите на трети страни (като например задължението да се създадат схеми за подаване на сигнали в случай на нарушения по закона Шарбан-Оксли в САЩ) не се включват в това основание. За да бъде валидно, законовото задължение, произтичащо от правото на трета страна ще трябва да бъде официално признато и ратифицирано в правния ред на съответната държава членка, тоест под формата на международно споразумение; и

(ii) „ясно и конкретно“ и предвидимо за прилагане спрямо физическите лица. Съображения 41 и 45 от GDPR изясняват, че релевантното „законово задължение“ не трябва да бъде закрепено, което би могло да има практически последствия по отношение на държави с правна система по общото право – би било достатъчно да отговаря на теста за „яснота и конкретност“. Правното задължение може да покрива няколко дейности по обработването, осъществявани от администратора, така че невинаги е необходимо да се идентифицира специално правно задължение за всяка отделна дейност[xiv].

Работната група по чл. 29 е посочила, че за да се приложи това правно основание, администраторът трябва да няма избор дали да изпълни задължението. Следователно доброволни многостранни ангажименти и публично-частни партньорства, по които се обработват данни извън изискваните по закон, не се покриват от това правно основание.[xv] Законовото задължение като основание за обработване на личните данни трябва да се прилага на основата на нормативни актове, отнасящи се изрично до характера и обекта на обработване[xvi].

Работната група по чл. 29 посочва, че законодателството може в някои случаи да зададе само обща цел, докато по-специфичните задължения да са установени на друго ниво (например в подзаконови актове или с обвързващи решения на държавен орган). Според Работната група по чл. 29, това също би могло да доведе до законово задължение, стига характерът и обектът на обработване да са добре определени и да са на въз основа на подходящо правно основание[xvii].

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

2.3.2. Приложимост по отношение на дейностите на местните власти

На практика това правно основание е едно от най-съотносимите по отношение на лични данни, обработвани от местните власти. То покрива всички ситуации, свързани с предоставянето на административни услуги и улесняване на изпълнението на законови задължения на гражданите и изпълнението на специфични задължения на местните власти в качеството им на работодатели. Това основание ще се прилага в следните ситуации:

- събиране на данни от местни власти за глоби за паркиране на неразрешени места;
- докладване на информация за трудовото възнаграждение за служители на местните власти на осигурителни и данъчни органи[xviii].

2.4. Защита на жизненоважни интереси

2.4.1. Значение и правни изисквания

Това правно основание трябва да се тълкува стеснително. Работната група по чл. 29 също отбелязва, че основанието защита на жизненоважните интереси трябва да се прилага ограничено[xix]. Понятието „жизненоважен интерес“ е неразривно свързано с непосредствена заплаха за основните права и блага на едно лице (живот, здраве, телесна неприкосновеност и други). В правната доктрина се отбелязва, че трябва законосъобразното обработване на лични данни на това правно основание следва да е жизненоважно за оцеляването на лицето[xx]. Според разясненията на Работната група по чл. 29 по старата Директива 95/46, заплахата трябва да е непосредствена, тоест събирането и обработването на лични данни в голям мащаб за чисто превантивни цели не би могло да попадне под това основание[xxi]. Съображение 46 от GDPR изрично дава възможност обработването на това основание за хуманитарни цели, включително при наблюдение на епидемии и тяхното разпространение или в ситуации на хуманитарна криза, в частност при природни бедствия и аварии (в тези случаи може да има припокриване между обществен интерес и жизненоважни интереси). Следователно, строгото разбиране, наложено от Работната група по чл. 29, може да бъде „омекотено“ за в бъдеще.

Трябва също да се отбележи, че по старата Директива 95/46 правното основание „защита на жизненоважен интерес“ се отнасяше само за интерес на физическото лице. В GDPR това основание има по-широк обхват – жизненоважният интерес може да бъде или на субекта на данни, или на друг лице. GDPR изрично изисква обработването на лични данни, основано на жизненоважен интерес на друго лице, по принцип да се осъществява само когато обработването не може очевидно да попадне под друго правно основание. С други думи, на основаването

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

на обработването за защита на жизненоважни интереси трябва да се гледа като на „последна възможност“ за администраторите.

2.4.2. Приложимост по отношение на дейностите на местните власти

Възможността да се приложи това основание в контекста на дейностите на местните власти е доста ограничена. Това основание теоретично би могло да се приложи в ограничен брой случаи, например да обоснове обработването на данни на служители или граждани в случай на извънредни ситуации, възникнали в юрисдикцията на местните власти, и ако няма друго правно основание за такова обработване (например законово задължение или упражняване на официални правомощия).

2.5. Изпълнение на задача от обществен интерес или при упражняването на официални правомощия

2.5.1. Значение и правни изисквания

Задачата или правомощието на администратора трябва да е установено в правото на ЕС или в правото на държавата членка, на която администраторът е подвластен. Задачи от обществен интерес на трета страна или при изпълнението на правомощия по чуждо право не попадат в обхвата на тази разпоредба по старата Директива 95/46[xxii] и този подход е продължен и в GDPR.

Аналогът на тази разпоредба по старата Директива покрива две различни ситуации:

(i) когато администраторът има официални правомощия или задача от обществен интерес (но не е задължен да обработва данни, напр. в хипотеза на оперативна самостоятелност).

(ii) когато администраторът няма официални правомощия, но трето лице с подобни правомощия изисква от него да предостави данни[xxiii].

В GDPR втората хипотеза е отпаднала, тоест в ситуации, в които данните се предоставят на трета страна с официални правомощия, това вече не е валидно основание за обработване на данни. С други думи, ситуациите, в които администраторът може да разчита на това правно основание, са стеснени.

Официалните правомощия или задачата от обществен интерес обикновено трябва да се предвидят в закони или други нормативни актове. Работната група по чл. 29 изрично е посочила, че по GDPR това правно основание трябва да бъде тълкувано по начин, който позволява на публичните власти известна гъвкавост, за да се осигури правилното им управление и функциониране. Следователно,

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

обработването на лични данни по такива дейности – по управление и функциониране - трябва се основава на легитимния интерес на администратора[xxiv].

Последно, но не по важност, трябва да се отбележи, че субектите имат право да възразят на обработване, основано на това правно основание. В тежест на администратора е да докаже, че има такива надделяващи легитимни основания да обработва данни[xxv].

2.5.2. Приложимост по отношение на дейностите на местните власти

Заедно с законовото задължение по чл. 6, буква „в“ от GDPR, задачата от обществен интерес/упражняването на официални правомощия е едно от най-важните правни основания за дейностите на местните власти. Примери за приложимостта на това основание, дадени от Работната група по чл. 29, са:

- данъчен орган, който събира и обработва данъчни декларации, за да установи и провери размера на данъка, който трябва да се плати – по аналогия това основание се отнася за местните власти, когато събират местни такси;
- местен орган по управлението (например община), натоварен със задължението да управлява библиотечни услуги, училища, местен басейн.

2.6. Легитимни интереси

2.6.1. Значение и правни изисквания

Правното основание „легитимни интереси“ съдържа два елемента:

(i) Легитимни интереси на администратора/трети лица:

a. понятието „интерес“ е дефинирано от Работната група по чл. 29 като по-голям материален интерес, който администраторът би могъл да има от обработването, или ползите, които той или обществото може да извлече[xxvi]. Интересът може да се отнася до облагодетелстване на обществото като цяло или само на съответния администратор/трето лице;

b. концепцията „легитимност“ е неразривно свързана със съответствието със закона – и законите за защита на личните данни, и законите, приложими към съответните дейности на администратора. С други думи, всяка незаконна цел, преследвана от администратора/трето лице, би изключила приложението на това правно основание. Работната група по чл. 29 е направила неизчерпателен списък на най-срещаните ситуации, в които легитимният интерес може да се приложи по старата Директива 95/46. Областите варират от реклама / дейности по привличане на вниманието (директен маркетинг, реклами или непоискани нетърговски

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

съобщения, включително за политически и дарителски кампании) до обществено-полезни дейности (например системи за подаване на сигнали, упражняване на правата на свобода на изразяване или на информация или за превенция на измами, неправомерно използване на услуги и пране на пари).

(ii) Легитимният интерес трябва да има преимущество пред интересите, основните права и свободи на физическите лица = трябва да се приложи тест на баланса във всеки отделен случай. Изискването е неразривно свързано с принципа за пропорционалност. Въпреки че администраторът/ третата страна може да има легитимен интерес да извършва обработването, то може да е диспропорционално (например съответното обработване може да е твърде навлизащо в личната сфера, в твърде голям мащаб, без надлежни ограничения и предпазни мерки и други) , като в такъв случай обработването не би било обосновано като законно. Работната група по чл. 29 е отбелязала, че измежду факторите, необходими да се направи тест на баланса, са:

a. преценка на легитимния интерес на администратора;
b. въздействие върху субекта на данни;
c. предварителен баланс; и
d. допълнителни мерки, приложени от администратора, за да предотврати всякакво неправомерно въздействие върху лицата[xxvii].

2.6.2. Приложимост по отношение на дейностите на местните власти

GDPR значително намалява приложимостта на основанието легитимен интерес в рамките на дейностите на публичните власти. GDPR изрично постановява, че това правно основание не трябва да се прилага към обработване, извършено от публични власти при упражняване на техните задачи. Логиката зад тази разпоредба е, че на публичните власти трябва да им бъде възложено със закон или друг нормативен акт да упражняват задачите си.

Следователно, препоръчва се местните власти, които разчитат на легитимен интерес за обработване на лични данни, да преосмислят кое друго основание за обработване на лични данни е по-подходящо да бъде приложено (задачи от обществен интерес/упражняване на официални правомощия).

Въпреки това, легитимният интерес все пак би могъл да се приложи от местните власти като валидно правно основание за вътрешни процеси – например дейности, свързани с човешки ресурси.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

3. ЗАКЛЮЧЕНИЕ И ПРАКТИЧЕСКИ СЪВЕТИ

Умението да се определи кое правно основание е приложимо към коя дейност по обработването е от изключителна важност за всеки администратор, за да може да се осигури законносъобразност на обработването. Още повече, че това, кое правно основание се прилага към всяка една цел на обработване, е сред от ключовите елементи на принципа за прозрачност, тъй като той изрично установява, че тази информация трябва да се предостави на всяко лице от администратора (чл. 13 и чл. 14 GDPR). Следователно, и администраторите от публичния, и администраторите от частния сектор, трябва да са напълно наясно със значението на всяко от правните основания в чл. 6 от GDPR и съответните им приложни полета. Регламентът не въвежда нови правни основания, а по-скоро изменя изискванията и условията за приложимостта на вече съществуващите (съгласие, легитимни интереси). Във всеки случай, да се идентифицира правилното правно основание е първата стъпка към осигуряване на съответствие с GDPR в рамките на една организация. В доктрината се посочва, че разумният администратор на лични данни трябва да предприеме необходимите стъпки, за да гарантира, че в случай, че надзорният орган поиска доказателства, по всяко време може да посочи на кое основание разчита за обработването и че лицата са правилно информирани за него[xxviii].

4. ВЪНШНИ ИЗТОЧНИЦИ И ЛИНКОВЕ

Книги

- **Voigt, CTP., von dem Bussche, A.**, The EU General Data Protection Regulation (GDPR) – A Practical Guide, Springer International Publishing (2017);
- **Boardman, R., Mullock, J., Mole, A.** Bird & Bird Guide to General Data Protection Regulation (2016);
- **EU** General Data Protection Regulation (GDPR). An Implementation and Compliance Guide, IT Governance Publishing, Cambridgeshire (2016);
- **European** Data Protection. Law and Practice, Executive Editor: Edurado Ustaran, CIPP/E, Partner, Hogan Lovells, IAPP (2018);

Документи на работната група по чл. 29

- WP29, Guidelines on Consent under Regulation 2016/679, WP 259;
- WP29, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, WP 217;

Интернет връзки

- http://europa.eu/rapid/press-release_IP-18-386_en.htm

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

- https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en
- https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/grounds-processing/when-can-personal-data-be-processed_en
- https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/grounds-processing/what-does-grounds-legitimate-interest-mean_en
- https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/grounds-processing/when-consent-valid_en
- https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/grounds-processing/does-consent-given-25-may-2018-continue-be-valid-once-gdpr-starts-apply-25-may-2018_en
- https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/grounds-processing/what-if-somebody-withdraws-their-consent_en
- https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/grounds-processing/what-if-somebody-withdraws-their-consent_en

5. ПРЕПРАТКИ

[i] Работна група по чл. 29, Guidelines on Consent under Regulation 2016/679, WP 259, стр. 6.
[ii] Работна група по чл. 29, Guidelines on Consent under Regulation 2016/679, WP 259, стр. 11-12.
[iii] Повече информация относно профилиране е достъпна в Работна група по чл. 29 Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (проект).
[iv] Работна група по чл. 29, Guidelines on Consent under Regulation 2016/679, WP 259, стр. 13.
[v] EU General Data Protection Regulation (GDPR). An Implementation and Compliance Guide, IT Governance Publishing, Cambridgeshire (2016), стр. 189-190.
[vi] Работна група по чл. 29, Guidelines on Consent under Regulation 2016/679, WP 259, стр. 7.
[vii] Примерът е даден от Работната група по чл. 29, Guidelines on Consent under Regulation 2016/679, WP 259, стр. 7.
[viii] Работна група по чл. 29 Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, WP 217, стр. 16-17.
[ix] Пак там, стр. 16.
[x] Voigt, CTP., von dem Bussche, A., The EU General Data Protection Regulation (GDPR) – A Practical Guide, Springer International Publishing (2017), стр. 102.
[xi] European Data Protection. Law and Practice, Executive Editor: Edurado Ustaran, CIPP/E, Partner, Hogan Lovells, IAPP (2018), стр. 118
[xii] Работна група по чл. 29 Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, WP 217, стр. 16.
[xiii] Пак там, стр. 20.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

[xiv] Boardman, R., Mullock, J., Mole, A. Bird & Bird Guide to General Data Protection Regulation (2016), стр. 10.
[xv] Работна група по чл. 29 Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, WP 217, стр. 19.
[xvi] Пак там, стр. 19.
[xvii] Пак там, стр. 20.
[xviii] Пак там, стр. 19.
[xix] Пак там, стр. 20.
[xx] European Data Protection. Law and Practice, Executive Editor: Edurado Ustaran, CIPP/E, Partner, Hogan Lovells, IAPP (2018), стр. 119.
[xxi] Работна група по чл. 29 Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, WP 217, стр. 20-21.
[xxii] Пак там, стр. 21.
[xxiii] Пак там, стр. 21.
[xxiv] Работна група по чл. 29 Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, WP 217, стр. 23.
[xxv] European Data Protection. Law and Practice, Executive Editor: Edurado Ustaran, CIPP/E, Partner, Hogan Lovells, IAPP (2018), стр. 119.
[xxvi] Работна група по чл. 29, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, WP 217, стр. 24.
[xxvii] Пак там, стр. 33.
[xxviii] European Data Protection. Law and Practice, Executive Editor: Edurado Ustaran, CIPP/E, Partner, Hogan Lovells, IAPP (2018), стр. 122.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

ProLegis

Обработване на специална категория данни

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

ProLegis

Съдържание

1. Правна рамка 4
   1.1. Харта на основните права на ЕС 4
   1.2. Общ регламент за защита на данните (GDPR) 4
2. СПЕЦИАЛНИ КАТЕГОРИИ ЛИЧНИ ДАННИ СПОРЕД GDPR 10
   2.1. Защо някои категории лични данни са определени като специални? 10
   2.2. Видове специални категории лични данни 11
   2.3. Лични данни, свързани с присъди и нарушения 13
3. ПРАВНИ ОСНОВАНИЯ ЗА ОБРАБОТВАНЕ НА СПЕЦИАЛНИ КАТЕГОРИИ ЛИЧНИ ДАННИ 14
   3.1. Изрично съгласие 14
   3.2. Задължения / специални права в областта на трудовото право, социалното осигуряване и социалната закрила 14
   3.3. Жизненоважни интереси на субекта на данни или друго физическо лице 15
   3.4. Обработване на лични данни от нестопанска организация с политическа, философска, религиозна или синдикална цел 15
   3.5. Данните са явно направени публично достояние от субекта на данните .. 16
   3.6. Установяване, упражняване или защита на правни претенции, когато съдилища действат в качеството си на правораздаващ орган 16
   3.7. Важен обществен интерес въз основа на правото на ЕС или на държавата-членка 17
   3.8. Превантивна или трудова медицина, оценка на работоспособността на служителя, медицинска диагноза, предоставяне на здравни или социални грижи или лечение 17
   3.9. Обществен интерес в областта на общественото здраве 18
   3.10. Обработване за целите на архивирането в обществен интерес, за целите на научни или исторически изследвания или за статистически цели 18
   3.11. Други хипотези в законодателството на държавите-членки 18
4. ЗАКЛЮЧЕНИЕ И ПРАКТИЧЕСКИ СЪВЕТИ GDPR 19

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

5. ВЪНШНИ ИЗТОЧНИЦИ И ИНТЕРНЕТ ЛИНКОВЕ 19
Книги 19
Документи на работната група по член 29 20
Интернет връзки 20
6. Препратки 20

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

1. Правна рамка

1.1. Харта на основните права на ЕС

Член 8

Защита на личните данни

1. Всеки има право на защита на личните данни, отнасящи се до нея/него.

2. Тези данни трябва да бъдат обработвани справедливо за конкретните цели и въз основа на съгласието на съответното лице или на друга легитимен принцип, предвиден в закона. Всеки има право на достъп до събраните данни, отнасящи се до него, и правото да бъдат поправени.

3. Съответствието с тези правила подлежи на контрол от независим орган.

1.2. Общ регламент за защита на данните (GDPR)

Съображение (51)

На личните данни, които по своето естество са особено чувствителни от гледна точка на основните права и свободи, се полага специална защита, тъй като контекстът на тяхното обработване би могъл да създаде значителни рискове за основните права и свободи. Посочените лични данни следва да включват личните данни, разкриващи расов или етнически произход, като използването на понятието „расов произход“ в настоящия регламент не означава, че Съюзът приема теориите, които се опитват да установят съществуването на отделни човешки раси. Обработването на снимки не следва систематично да се счита за обработване на специални категории лични данни, тъй като снимките се обхващат от определението за биометрични данни единствено когато се обработват чрез специални технически средства, позволяващи уникална идентификация или удостоверяване на автентичността на дадено физическо лице. Тези лични данни не следва да се обработват, освен ако обработването не е разрешено в определени случаи, предвидени в настоящия регламент, като се има предвид, че в правото на държавите членки могат да бъдат определени специфични разпоредби за защита на данните с цел да се адаптира прилагането на съдържащите се в настоящия регламент правила за спазване на правно задължение или за изпълнение на задача от обществен интерес или свързана с упражняването на официални правомощия, предоставени на администратора на лични данни. В допълнение към конкретните изисквания за такова обработване следва да се прилагат общите принципи и другите правила, залегнали в настоящия регламент, по-специално по отношение на условията за законосъобразно обработване. Дерогации от

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

общата забрана за обработване на такива специални категории лични данни следва изрично да бъдат предвидени, inter alia, когато субектът на данните даде изричното си съгласие или във връзка с конкретни нужди, по-специално когато обработването се извършва в хода на законната дейност на някои сдружения или фондации, чиято цел е да се позволи упражняването на основните свободи.

Съображение (52)

Дерогация от забраната за обработване на специални категории лични данни също следва бъде разрешена, когато е предвидена в правото на Съюза или правото на държава членка, и при подходящи гаранции, така че да бъдат защитени личните данни и други основни права, когато съображения, свързани с обществения интерес, оправдават това, по-специално обработването на лични данни в областта на трудовото право, правото в областта на социалната закрила, включително пенсиите, както и за целите на сигурността, наблюдението и предупрежденията в сферата на здравеопазването, предотвратяването или контрола на заразните болести и други сериозни заплахи за здравето. Такава дерогация може да се извърши за здравни цели, включително общественото здраве и управлението на здравните услуги, особено с цел да се гарантират качеството и рентабилността на използваните процедури за уреждане на искове за обезщетения и услуги в системата за здравно осигуряване, или за целите на архивирането в обществен интерес, за целите на научни или исторически изследвания, или за статистически цели. Чрез дерогация следва да се даде възможност да се обработват и такива лични данни, когато е необходимо, с цел установяване, упражняване или защита на правни претенции, независимо дали това е в рамките на съдебна, административна или друга извънсъдебна процедура

Съображение (53)

Специални категории лични данни, които се нуждаят от по-голяма защита, могат да бъдат обработвани единствено за здравни цели, когато е необходимо тези цели да бъдат постигнати в полза на отделни физически лица и на обществото като цяло, по-специално в рамките на управлението на услугите и системите за здравеопазване или социални грижи, включително обработването от страна на органите за управление и от централните национални здравни органи на такива данни за целите на контрола на качеството, информацията за управлението и общото наблюдение на национално и местно равнище на системата за здравеопазване или социални услуги, както и за осигуряване на непрекъснатост на здравното обслужване или на социалните услуги и на

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

трансграничното здравно обслужване или за целите на сигурността, наблюдението и предупрежденията в сферата на здравеопазването, или за целите на архивирането в обществен интерес, за целите на научни или исторически изследвания или за статистически цели въз основа на правото на Съюза или националното право, което трябва да отговаря на цел от обществен интерес, както и за проучванията в областта на общественото здраве, провеждани в обществен интерес. Поради това настоящият регламент следва да предвижда хармонизирани условия за обработването на специални категории лични данни за здравословното състояние по отношение на специфични нужди, по-специално когато обработването на тези данни се извършва за определени цели, свързани със здравето, от лица, обвързани от правното задължение за професионална тайна. Правото на Съюза или националното право следва да предвижда конкретни и подходящи мерки за защита на основните права и личните данни на физическите лица. Държавите членки следва да разполагат с възможност да запазят или да въведат допълнителни условия, включително ограничения, по отношение на обработването на генетични, биометрични или данни за здравословното състояние. Това обаче не следва да възпрепятства свободното движение на лични данни в рамките на Съюза, когато тези условия се прилагат за трансгранично обработване на такива данни.

Съображение (54)

Обработването на специални категории лични данни може да е необходимо по съображения от обществен интерес в областта на общественото здраве, без съгласието на субекта на данните. Такова обработване следва да бъде предмет на подходящи и конкретни мерки с оглед защита на правата и свободите на физическите лица. В този контекст понятието „обществено здраве“ следва да се тълкува по смисъла на Регламент (ЕО) № 1338/2008 на Европейския парламент и на Съвета и означава всички елементи, свързани със здравето, а именно здравословно състояние, включително заболеваемост и инвалидност, решаващи фактори, които оказват влияние върху това здравословно състояние, потребности от здравно обслужване, средства, отделени за здравно обслужване, предоставяне на здравни грижи и всеобщ достъп до тях, разходи и финансиране на здравното обслужване, както и причини за смъртност. Такова обработване на данни за здравето по съображения от обществен интерес не следва да води до обработването на лични данни за други цели от трети страни като работодатели или застрахователни дружества и банки.

Съображение (55)

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

Освен това обработването на лични данни от официални органи за постигането на целите, определени в конституционното право или в международното публично право, на официално признати религиозни сдружения се извършва по съображения от обществен интерес.

Съображение (56)

Когато демократичната система в дадена държава членка предполага по време на предизборна дейност политическите партии да събират лични данни за политическите възгледи на гражданите, обработването на тези данни може да бъде разрешено по съображения от обществен интерес, при условие че са предвидени подходящи гаранции.

Член 4

Дефиниции

За целите на настоящия Регламент:

11)„съгласие на субекта на данните“означава всяко свободно изразено, конкретно, информирано и недвусмислено указание за волята на субекта на данните, посредством изявление или ясно потвърждаващо действие, което изразява съгласието му свързаните с него лични данни да бъдат обработени;

12)„нарушение на сигурността на лични данни“ означава нарушение на сигурността, което води до случайно или неправомерно унищожаване, загуба, промяна, неразрешено разкриване или достъп до лични данни, които се предават, съхраняват или обработват по друг начин;

13)„генетични данни“ означава лични данни, свързани с наследени или придобити генетичните белези на дадено физическо лице, които дават уникална информация за отличителните черти или здравето на това физическо лице и които са получени, по-специално, от анализ на биологична проба от въпросното физическо лице;

Член 9

Обработване на специални категории лични данни:

1. Забранява се обработването на лични данни, разкриващи расов или етнически произход, политически възгледи, религиозни или философски убеждения или членство в синдикални организации, както и обработването на генетични данни, биометрични данни за целите единствено на

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

идентифицирането на физическо лице, данни за здравословното състояние или данни за сексуалния живот или сексуалната ориентация на физическото лице.

2. Параграф 1 не се прилага, ако е налице едно от следните условия:

а) субектът на данни е дал своето изрично съгласие за обработването на тези лични данни за една или повече конкретни цели, освен когато в правото на Съюза или правото на държава членка се предвижда, че посочената в параграф 1 забрана не може да бъде отменена от субекта на данни;

б) обработването е необходимо за целите на изпълнението на задълженията и упражняването на специалните права на администратора или на субекта на данните по силата на трудовото право и правото в областта на социалната сигурност и социалната закрила, дотолкова, доколкото това е разрешено от правото на Съюза или правото на държава членка, или съгласно колективна договореност в съответствие с правото на държава членка, в което се предвиждат подходящи гаранции за основните права и интересите на субекта на данните;

в) обработването е необходимо, за да бъдат защитени жизненоважните интереси на субекта на данните или на друго физическо лице, когато субектът на данните е физически или юридически неспособен да даде своето съгласие;

г) обработването се извършва при подходящи гаранции в хода на законните дейности на фондация, сдружение или друга структура с нестопанска цел, с политическа, философска, религиозна или синдикална цел, при условие че обработването е свързано единствено с членовете или бившите членове на тази структура или с лица, които поддържат редовни контакти с нея във връзка с нейните цели, и че личните данни не се разкриват без съгласието на субектите на данните;

д) обработването е свързано с лични данни, които явно са направени обществено достояние от субекта на данните;

е) обработването е необходимо с цел установяване, упражняване или защита на правни претенции или винаги, когато съдилищата действат в качеството си на правораздаващи органи;

ж) обработването е необходимо по причини от важен обществен интерес на основание правото на Съюза или правото на държава членка, което е пропорционално на преследваната цел, зачита същността на правото на защита на данните и предвижда подходящи и конкретни мерки за защита на основните права и интересите на субекта на данните;

з) обработването е необходимо за целите на превантивната или трудовата медицина, за оценка на трудоспособността на служителя, медицинската диагноза, осигуряването на здравни или социални грижи или лечение, или за целите на управлението на услугите и системите за здравеопазване или

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

социални грижи въз основа на правото на Съюза или правото на държава членка или съгласно договор с медицинско лице и при условията и гаранциите, посочени в параграф 3;

и) обработването е необходимо от съображения от обществен интерес в областта на общественото здраве, като защитата срещу сериозни трансгранични заплахи за здравето или осигуряването на високи стандарти за качество и безопасност на здравните грижи и лекарствените продукти или медицинските изделия, въз основа на правото на Съюза или правото на държава членка, в което са предвидени подходящи и конкретни мерки за гарантиране на правата и свободите на субекта на данните, по-специално опазването на професионална тайна;

й) обработването е необходимо за целите на архивирането в обществен интерес, за научни или исторически изследвания или за статистически цели съгласно член 89, параграф 1, на основание правото на Съюза или правото на държава членка, което е пропорционално на преследваната цел, зачита същността на правото на защита на данните и предвижда подходящи и конкретни мерки за защита на основните права и интересите на субекта на данните.

3. Личните данни, посочени в параграф 1, могат да бъдат обработвани за целите, посочени в параграф 2, буква з), когато въпросните данни се обработват от или под ръководството на професионален работник, обвързан от задължението за професионална тайна по силата на правото на Съюза или правото на държавата членка или правилата, установени от националните компетентни органи или от друго лице, също обвързано от задължение за тайна по силата на правото на Съюза или правото на държавата членка или правилата, установени от националните компетентни органи.

4. Държавите членки могат да запазят или да въведат допълнителни условия, включително и ограничения, по отношение на обработването на генетични данни, биометрични данни или данни за здравословното състояние.

Член 10

Обработване на лични данни, свързани с присъди и нарушения

Обработването на лични данни, свързани с присъди и нарушения или със свързаните с тях мерки за сигурност, въз основа на член 6, параграф 1, се извършва само под контрола на официален орган или когато обработването е разрешено от правото на Съюза или правото на държава членка, в което са предвидени подходящи гаранции за правата и свободите на субектите на данни.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

Пълен регистър на присъдите по наказателни дела се поддържа само под контрола на официален орган.

2. СПЕЦИАЛНИ КАТЕГОРИИ ЛИЧНИ ДАННИ СПОРЕД GDPR

2.1. Защо някои категории лични данни са определени като специални?

Дори в хода на изготвянето на първия правен акт на ЕС, посветен на защитата на личните данни - Директива 95/46 - Европейската комисия подчертава, че обработването на някои категории лични данни може да доведе до по-голям риск за основните права и свободи на европейските граждани[i]. По този начин е установена обща забрана за обработването на такива "рискови" категории лични данни. Те се определят като "специални категории лични данни", но в практиката често се наричат още "чувствителни данни" поради деликатното им естество, засягащо личната сфера на всеки индивид[ii]. Тези данни могат да бъдат обработвани само при изключителни обстоятелства, изчерпателно изброени в законодателството за защита на данните на държавите-членки.

GDPR продължава този подход, но разширява обхвата на специалните категории лични данни и предвижда някои нови изключения (правни основания), които дават право на администраторите да обработват такива данни.

Трябва да се отбележи, че различните видове данни имат различно въздействие върху отделните хора. Кои данни се определят като чувствителни се основава на обективен, а не на субективен принцип. С други думи, някой може да сметне, че данните, свързани с финансово състояние, историята на дисциплинарни санкции или социалноосигурителен номер, са чувствителни. И все пак, ако тези данни не са припознати от европейския законодател като чувствителни, те няма да попаднат в специален режим за обработване, независимо от чувствителното си естество от субективна гледна точка[iii].

В доктрината се посочва, че изборът, кои категории лични данни следва да бъдат определени като специални, е значително повлиян от законите за борба с дискриминацията, което обяснява защо такива данни като социалноосигурителни номера и данни за кредитни карти (които, ако бъдат обект на злоупотреба, биха могли да причинят сериозна вреда на лицата) не са дефинирани като чувствителни.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

2.2. Видове специални категории лични данни

Съгласно чл. 9, ал. 1 от GDPR, следните видове лични данни попадат в обхвата на специалните категории лични данни(чувствителни данни):

- лични данни, разкриващи расов или етнически произход = тези категории лични данни са определени като чувствителни, тъй като водят до висок риск от дискриминация. В правната доктрина са дадени следните примери за това какви данни могат да попаднат в тази категория: собствено и фамилно име на лицето, място на раждане, родния му език или имената на родителите му, които при комбиниране биха позволили да се направят заключения за неговия произход[iv];
- политически възгледи = тези данни се ползват от специална защита, защото са свързани с правото на гражданите да формират свободно мнение по отношение на политиката и в крайна сметка да участват (активно като политици и/или пасивно като електорат и членове на гражданското общество) в политическия живот на страната. Примерите за такива данни включват информация относно членството в политическите партии, информация относно присъединяването към всякакви петиции, участие в демонстрации, политическо събиране или подобни събития, информация относно подкрепата за дадена политическа идея или нейното отхвърляне[v];
- религиозни или философски убеждения = тези категории данни са тясно свързани със свободата на съвестта и религията, т.е. свободата да решаваме дали да вярваме в трансцеденталните сили, които предопределят ежедневието ни и дали да го проявяваме открито или не. Историята на човечеството е изпълнена с примери, в които насилие е породено въз основа на религиозни различия, поради което такива данни следва да бъдат специално защитени съгласно правилата за защита на данните;
- членство в синдикални организации = информация за такива членове е чувствителна, тъй като създава риск от дискриминационно третиране в областта на трудовото право. Европейските граждани имат свободата на колективно договаряне и следователно не трябва да се третират неравностойно на базата на тяхната професионална принадлежност[vi];
- генетични данни = нова категория, въведена от GDPR като тип чувствителни данни. GDPR ги определя като "данни, свързани с наследствените или придобитите генетични характеристики на физическо лице, които дават уникална информация за физиологията или здравето на това физическо лице и които произтичат по-специално от анализ на биологична проба от дадено физическото лице. Някои държави-членки вече са установили

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

статуса им на чувствителни[vii], но за първи път GDPR го въвежда на европейско равнище. Генетичните данни трябва да бъдат защитени, тъй като тези видове данни се отнасят не само до съответното физическо лице, но и могат да засегнат неопределен кръг лица, които са част от родословието на определено физическо лице (включително данни за починали лица, данни за деца и т.н.). Освен това подробният анализ на такива данни може да разкрие други видове чувствителна информация, като психологически данни или данни относно здравето (напр. предразположеност към болести, уязвимост и т.н.);

- биометрични данни за целите единствено на идентифицирането на физическо лице = такива видове данни следва да се ползват от специално ниво на защита, тъй като позволяват на администраторите недвусмислено да идентифицират дадено физическо лице въз основа на неговите физически или поведенчески характеристики: пръстови отпечатъци, лицево разпознаване, ирис, ретина , съдови модели, ДНК, реч, почерк, начин на използване на клавиатура и т.н.). Обработването на подобни видове данни става все по-често при въвеждането на различни технологични решения (например системи за контрол на достъпа до помещения, системи за идентификация на устройства като мобилни телефони, таблети и т.н.). Ето защо е необходимо този тип обработване на лични данни да бъде по-ограничено и и контролирано. Това е и причината за включването на тези данни в списъка на "чувствителните" в GDPR. Противно на практиките, установени в някои държави-членки, обработването на фотографии не се счита автоматично за обработване на чувствителни данни. Снимките попадат в обхвата на биометрични данни, само ако позволяват уникалната идентификация или автентификация на дадено (например снимка електронен паспорт или друг вид документ за самоличност)[viii];
- данни за здравословното състояние или данни за сексуалния живот или сексуалната ориентация на физическото лице = тези данни са много чувствителни, тъй като засягат най-интимните аспекти на живота на индивида. Освен това, информацията относно сексуалния живот и сексуалната ориентация носи риск от дискриминация, манипулация и т.н. В теорията се посочва, че тези данни включват и инвидуализирането на партньора/ите на дадено лице[ix].

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

2.3. Лични данни, свързани с присъди и нарушения

Личните данни, свързани с наказателни присъди и нарушения или свързани с тях мерки за сигурност, не са определени като специална категория лични данни. Въпреки това, законодателството на някои държави-членки ги третира като чувствителни[x]. Независимо от това, този вид обработването на такава лична информация крие риск от неравно третиране (например на пазара на труда), поради което тези данни също са обект на специални правила за законосъобразно обработване. GDPR не въвежда значителни новости в сравнение със старата Директива 95/46 по отношение на данните за наказателни присъди и нарушения. В същото време, предвид факта, че правилата на Директивата са транспонирани по различен начин в държавите-членки, GDPR въвежда хармонизиран подход на ниво ЕС към такива данни. Съгласно нормата на чл. 10 от GDPR, тези данни могат да бъдат обработвани въз основа на едно от основанията по чл. 6, при условие, че е налице едно от двете допълнителни алтернативни условия:

i) обработването трябва да бъде под контрола на официален орган;
ii) обработването е разрешено от законодателството на ЕС / държавата-членка, което предвижда подходящи гаранции за правата и свободите на субектите на данни.

Съществува неяснота относно тази разпоредба, тъй като не е ясно как посочените две допълнителни изисквания следва да се прилагат заедно с чл. 6. Консервативното тълкуване е, че частни организации или търговски дружества не могат да обработват такива данни, с други думи "в Регламента не предвидено на обработването на тези данни от частни организации и търговци"[xi]. Другото тълкуване е, че такъв тип данни могат да бъдат обработвани на всички възможни правни основания, при условие, че са изпълнени допълнителните условия (под контрола на официалните власти или ако това е позволено съгласно приложимото право). В доктрината се посочва, че тази разпоредба вероятно ще доведе до значителни национални отклонения[xii]. Макар че местните власти тук ще действат като публични органи и теоретично биха могли да оправдаят първото допълнително изискване за обработване (под контрола на държавната власт), все пак би било препоръчително внимателно да се проучи националната уредба кога такива видове данни могат да бъдат обработвани (особено в контекста на дейности, свързани с човешки ресурси и събиране на свидетелства за съдимост, тъй като тук съответните органи на местната власт действат като работодател, а не като орган на публичната власт и приложимостта на първото допълнително условие е под въпрос).

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

3. ПРАВНИ ОСНОВАНИЯ ЗА ОБРАБОТВАНЕ НА СПЕЦИАЛНИ КАТЕГОРИИ ЛИЧНИ ДАННИ

Общата забрана за обработване на специални категории лични данни не се прилага, при условие, че е налице едно от **алтернативните** условия, изброени по-долу:

3.1. Изрично съгласие

Изискванията, които трябва да бъдат спазени в GDPR, за да има валидно съгласие (свободно дадено, конкретно, информирано, недвусмислено), се прилагат във всеки случай на обработване на специална категория данни. Елементът "изрично" обаче не е дефиниран в GDPR. Работната група по член 29 посочва, че е необходимо изрично съгласие в ситуации, при които би могъл да възникне сериозен риск за защитата на данните и където е подходящо да се упражнява високо ниво на индивидуален контрол върху обработваните лични данни[xiii].

Терминът "изрично" се отнася до начина, по който се изразява съгласието на субекта на данните - субектът на данните следва да направи изрично изявление за съгласие[xiv]. Един от начините да се даде съгласие изрично е то да се потвърди писмено. В електронна среда могат да се приложат различни решения като например попълване на електронен формуляр, изпращане на имейл, качване на сканиран документ с подписа на субекта на данните или използване на електронен подпис. Подходящи биха били и всички други средства, които позволят на администратора да докаже изричното даване на съгласие от дадено физическо лице.

Предвид липсата на равнопоставеност между субектите на данни и местните власти, не е целесъобразно органите на местната власт основно да разчитат на изричното съгласие за обработване на специални категории лични данни (включително в отношенията с граждани и служители).

3.2. Задължения / специални права в областта на трудовото право, социалното осигуряване и социалната закрила

Това правно основание е от особена значимост за местните власти с оглед всички вътрешни процеси, свързани с човешки ресурси. Обработването на специални категории лични данни може да се случи на всеки етап от едно трудово правоотношение - от неговото възникване (процес на наемане на нов персонал), през изпълнението и изменението му и в крайна сметка до неговото прекратяване.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

Примери кога се случва подобно обработване включва проследяването на болнични и отпуски по майчинство, трудоустрояване, спазване на задължителни правила при предварителна закрила при уволнение и т.н.

Общите изисквания, въведени в GDPR за приложенията на това основание, са:

i) обработването трябва да е необходима, за да се изпълни задължение на администратора на данни или определено право на субекта на данни;
ii) това задължение / право следва да бъде установено в законодателството на ЕС / на държавите-членки или в колективен трудов договор;
iii) трябва да съществуват подходящи гаранции за основните права и интереси на субекта на данните.

С оглед обработването на специални категории данни на това правно основание, трябва да се спазва приложимото национално законодателство на държавата-членка. Тъй като трудовото законодателство е една от областите, където GDPR позволява на държавите-членки да приемат допълнително законодателство по отношение на защитата на личните данни (член 88), се препоръчва подход на местно равнище при прилагането на това основание.

3.3. Жизненоважни интереси на субекта на данни или друго физическо лице

Подобно на правното основание по чл. 6, ал. 1, б. "г" от GDPR, такава ситуация се отнася до обстоятелства на живот или смърт[xv]. Жизненоважният интерес може да бъде както на субекта на данните, така и на друго лице. Различното в сравнение с чл. 6 е, че администраторът носи тежестта да докаже наличието на допълнително условие, а именно, че "субектът на данните физически или юридически не е в състояние да даде съгласие". Тази формулировка предполага, че администраторът трябва първо да се опита да получи съгласието на субекта на данните[xvi].

3.4. Обработване на лични данни от нестопанска организация с политическа, философска, религиозна или синдикална цел

Възможността за обработване на чувствителни данни в рамките на това правно основание се предоставя на определени организации с нестопанска цел, като политически партии, фондации, църкви, други форми на философски, религиозни или синдикални организации. Тези организации могат да обработват чувствителни данни, ако:

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

i) тези данни се отнасят единствено до членове / бивши членове на организацията или до лица, които имат редовен контакт с него;
ii) обработването е в хода на законната им дейност;
iii) обработването се извършва във връзка със специфичните им цели;
iv) съществуват подходящи гаранции за правата на субекта на данните;
v) личните данни не се разкриват без съгласието на субектите на данните.

Други специфични изисквания могат да се предвидят в националното законодателство[xvii].

Това правно основание би имало почти никакво практическо приложение спрямо местните органи в хода на тяхната дейност.

3.5. Данните са явно направени публично достояние от субекта на данните

Ако личните данни са явно разкрити пред широката общественост от субекта на данните, се предполага, че той е отказал специалната защита, предоставена за такава информация. Във всеки случай решението за разкриване на такава информация следва да бъде резултат от свободния избор на лицето[xviii]. Такова разкриване може да има различни форми - данни от обществено достъпни регистри, уебсайтове, списъци, форуми или дори от профил в социална мрежа, достъпен без потребителски акаунт и т.н[xix]. Във всеки случай фактът, че тези данни са явно оповестени не освобождава администратора от задължението да спазва другите изисквания на GDPR - например спазване на принципите за защита на данните, защита на личните данни при проектиране и по подразбиране, предприемане на подходящи организационни и технически мерки за гарантиране на сигурността на данните и т.н.

3.6. Установяване, упражняване или защита на правни претенции, когато съдилища действат в качеството си на правораздаващ орган

В някои случаи обработването на „чувствителни данни“ може да е необходимо с оглед упражняването на правни претенции и защита на правни искове от администратора. Именно администраторът носи тежестта да докаже, че е такова обработване е необходимо, т.е. че има тясна и съществена връзка между обработването и целите[xx]. Такива ситуации могат да включват например обжалване пред административните съдилища на актове, издадени от месните власти, когато обработването на чувствителни данни е извършена в предходната административна процедура; трудови спорове, където здравните данни на

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

работниците и служителите трябва да са били взети предвид от органа на местната власт като работодател и т.н.

Освен това, обработването на лични данни в рамките на правораздавателната дейност на съдилищата може също така да включи обработване на специални категории лични данни.

3.7. Важен обществен интерес въз основа на правото на ЕС или на държавата-членка

Тази разпоредба на GDPR упълномощава държавите-членки да установят в своето национално законодателство конкретна хипотеза, при която могат да бъдат обработвани чувствителни данни, въз основа на важен обществен интерес.

Във всеки случай, за да се отговори на изискванията на GDPR, държавите-членки следва да гарантират, че:

i) дейностите по обработване са пропорционални на преследваната цел;
ii) същността на правото на защита на данните се спазва;
iii) приетото законодателство предвижда подходящи и специфични мерки за защита на основните права и интересите на субекта на данните.

Остава да се види как ще се използва тази възможност в бъдеще. Необходим е анализ на всеки отделен случай по отношение приложимото национално законодателство от местните власти, за да се определи дали те могат да се осланят на такива основания.

3.8. Превантивна или трудова медицина, оценка на работоспособността на служителя, медицинска диагноза, предоставяне на здравни или социални грижи или лечение

Забраната за обработване на специални категории лични данни не се прилага за дейности, свързани с медицински цели и социални грижи[xxi]. Такова обработване може да се извърши в различни области като трудова медицина, медицинска диагностика или предоставяне на услуги в областта на социалната или медицинската помощ. Такова обработване може да се извърши и въз основа на законодателството на ЕС или на държавата-членка, или по договор със здравен специалист[xxii]. Освен това чл. 9, ал. 3 от GDPR позволява обработването на чувствителни данни от лице, обвързано със задължение за пазене на професионална тайна.

Това правно основание се прилага спрямо обработването на лични данни от лекари, медицински сестри и други лица, участващи в предоставянето на здравни услуги[xxiii].

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

От практическа гледна точка тази разпоредба би позволила на органите на местната власт в качеството им на работодатели да осигурят трудова медицина като част от по-голямото им задължение за осигуряване на здравословни и безопасни условия на труд.

3.9. Обществен интерес в областта на общественото здраве

Съгласно съображение 54 от GDPR, "общественото здраве" следва да се тълкува по смисъла на Регламент (ЕО) № 1338/2008 на Европейския парламент, а именно - всички елементи, свързани със здравето: здравословно състояние, включително заболеваемост и инвалидност, решаващи фактори, които оказват влияние върху здравословното състояние, потребности от здравно обслужване, средства, предназначени за здравно обслужване, предоставяне на здравни грижи и всеобщ достъп до тях, разходи и финансиране на здравното обслужване, както и причините за смъртност.

Причините, които биха могли да оправдаят прилагането на това правно основание, биха могли да бъдат защитата срещу сериозни трансгранични заплахи за здравето или гарантирането на високи стандарти за качество и безопасност на здравните грижи, медицинските продукти или медицинските устройства[xxiv].

Такова обработване на данни за здравето по съображения от обществен интерес не следва да води до обработването на лични данни за други цели от трети страни като работодатели или застрахователни дружества и банки.

3.10. Обработване за целите на архивирането в обществен интерес, за целите на научни или исторически изследвания или за статистически цели

Обработването на специални категории данни за такива цели следва да се основава на законодателството на държавата-членка / законодателството на ЕС. GDPR изисква законодателните разпоредби, позволяващи такава обработка, да бъдат: пропорционални на преследваната цел, да зачитат същността на правото на защита на данните и да предвиждат подходящи и специфични мерки за защита на основните права и интереси на субекта на данните. Въведените предпазни мерки трябва да съответстват на чувствителния характер на съответните лични данни.

3.11. Други хипотези в законодателството на държавите-членки

Чл. 9, ал. 4 от GDPR упълномощава държавите-членки да въведат допълнителни условия или ограничения за обработването на някои от специалните категории лични данни, а именно: генетични данни, биометрични данни или данни

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

относно здравето. Следователно националното законодателство трябва да бъде наблюдавано в бъдеще при подобрен род дейности по обработване на специални категории данни.

4. ЗАКЛЮЧЕНИЕ И ПРАКТИЧЕСКИ СЪВЕТИ GDPR

За местните власти припознаването на факта, че някои категории лични данни заслужават специална защита, тъй като те по своята същност са свързани с най-интимните лични сфери и / или могат да доведат до риск от дискриминация. По общо правило обработването на такива данни е забранено, освен ако не са налице допълнителни условия (изключения от това правило).

Практическите аспекти, които биха могли да засегнат дейностите на органите на местната, са дейностите по обработване на данни за здравето на служителите. GDPR разрешава подобно обработване, но само ако то е задължително за администратора (или е право на субекта на данни) съгласно трудовото законодателство.

Данните за присъди и нарушения не се третират като специална категория, но също са под специален режим по GDPR. Ето защо практики при подбор на персонал, при които се изискват свидетелства за съдимост или извършване на обстойни проверки на бъдещи служители, следва да бъде преразгледана в светлината на GDPR.

5. ВЪНШНИ ИЗТОЧНИЦИ И ИНТЕРНЕТ ЛИНКОВЕ

Книги

- **Boardman, R., Mullock, J., Mole, A.** Bird & Bird Guide to General Data Protection Regulation (2016);
- **Ehmann, E., Helfrich, M.** EG Datenschutzrichtlinie: Kurzkommentar, Verlag Dr. Otto Schmidt, Koln, (1999)
- **Voigt, P., von dem Bussche, A.**, The EU General Data Protection Regulation (GDPR) – A Practical Guide, Springer International Publishing (2017);
- **EU** General Data Protection Regulation (GDPR). An Implementation and Compliance Guide, IT Governance Publishing, Cambridgeshire (2016);

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

- **European** Data Protection. Law and Practice, Executive Editor: Edurado Ustaran, CIPP/E, Partner, Hogan Lovells, IAPP (2018);

Документи на работната група по член 29

- WP29, Guidelines on Consent under Regulation 2016/679, WP 259;
- WP29, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, WP 217;

Интернет връзки

- http://europa.eu/rapid/press-release_IP-18-386_en.htm
- https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en
- https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/sensitive-data/what-personal-data-considered-sensitive_en
- https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/sensitive-data/under-what-conditions-can-my-company-organisation-process-sensitive-data_en

6. Препратки

[i] GDPR изрично използва термина „чувствителни данни“, вж. пример Съображение (10).
[ii] European Data Protection. Law and Practice, Executive Editor: Edurado Ustaran, CIPP/E, Partner, Hogan Lovells, IAPP (2018), стр. 123.
[iii] Voigt, P., von dem Bussche, A., The EU General Data Protection Regulation (GDPR) – A Practical Guide, Springer International Publishing (2017), стр. 111.
[iv] Пак там, стр. 111.
[v] Пак там, стр. 111.
[vi] У нас този тип лична информация е призната за чувствителни лични данни през 2005 г.
[vii] Boardman, R., Mullock, J., Mole, A. Bird & Bird Guide to General Data Protection Regulation (2016), стр. 18.
[viii] Voigt, P., von dem Bussche, A., The EU General Data Protection Regulation (GDPR) – A Practical Guide, Springer International Publishing (2017), стр. 111.
[ix] Boardman, R., Mullock, J., Mole, A. Bird & Bird Guide to General Data Protection Regulation (2016), стр. 19.
[x] EU General Data Protection Regulation (GDPR). An Implementation and Compliance Guide, IT Governance Publishing, Cambridgeshire (2016), стр. 196.
[xi] Boardman, R., Mullock, J., Mole, A. Bird & Bird Guide to General Data Protection Regulation (2016), стр. 19.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

[xii] Работна група по чл. 29, Guidelines on Consent under Regulation 2016/679, WP 259, стр. 18.
[xiii] Пак там, стр. 18.
[xiv] European Data Protection. Law and Practice, Executive Editor: Edurado Ustaran, CIPP/E, Partner, Hogan Lovells, IAPP (2018), стр. 126.
[xv] Пак там, стр. 126.
[xvi] Пак там, стр. 126 - 127.
[xvii] Voigt, P., von dem Bussche, A., The EU General Data Protection Regulation (GDPR) – A Practical Guide, Springer International Publishing (2017), стр. 113.
[xviii] Пак там, стр. 113
[xix] European Data Protection. Law and Practice, Executive Editor: Edurado Ustaran, CIPP/E, Partner, Hogan Lovells, IAPP (2018), стр. 127.
[xx] Пак там, стр. 128
[xxi] Пак там, стр. 129
[xxii] Пак там, стр. 129
[xxiii] Voigt, P., von dem Bussche, A., The EU General Data Protection Regulation (GDPR) – A Practical Guide, Springer International Publishing (2017), стр. 114.
[xxiv] Пак там, стр. 115

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

ProLegis

Назначаване, позиция и функции на длъжностните лица по защита на данните (ДЛЗД)

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

ProLegis

Съдържание

1. ПРАВНА РАМКА 4

Общ регламент за защита на данните (GDPR) 4

2. Назначаване на Длъжностно лице по защита на данните (ДЛЗД) 7

2.1. Задължително назначаване по GDPR 7

2.1.1. Публичен орган 7

2.1.2. Основните дейности на администратора/ обработващия […] изискват редовно и систематично мащабно наблюдение на субектите 8

2.1.3. Основните дейности на администратора или на обработващия лични данни се състоят в мащабно обработване на специални категории лични данни и данни относно присъди и нарушения 9

2.2. Други ситуации, в които се назначава ДЛЗД 9

2.2.1. Задължително назначаване по правото на ЕС/правото на държавата членка 9

2.2.2. Доброволно назначаване 10

2.3. Договорни отношения с ДЛЗД 10

2.3.1. Трудов договор 10

2.3.2. Договор за услуга 11

3. ПОЗИЦИЯ НА ДЛЗД 11

3.1. Участие във всички въпроси, свързани със защитата на личните данни .. 11

3.2. Осигуряване на нужните ресурси и на независимост 12

3.3. Конфликт на интереси 13

4. ФУНКЦИИ НА ДЛЗД 14

4.1. Наблюдение 14

4.2. Оценка на въздействието върху защитата на лични данни (ОВЗЛД) 14

4.3. Точка за контакт 14

4.4. Поддържане на регистри 15

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

5. ЗАКЛЮЧЕНИЕ И ПРАКТИЧЕСКИ СЪВЕТИ 15
6. ВЪНШНИ ИЗТОЧНИЦИ И ЛИНКОВЕ 16
Книги 16
Документи на Работната група по чл. 29 16
Интернет връзки 16
7. ПРЕПРАТКИ 16

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

1. ПРАВНА РАМКА

Общ регламент за защита на данните (GDPR)

Съображение (97)

Когато обработването на данни се извършва от публичен орган, с изключение на съдилища или съдебни органи, които действат в изпълнение на съдебните си функции, когато в частния сектор обработването се извършва от администратор, чиито основни дейности се състоят от операции по обработване, които изискват редовно и систематично мащабно наблюдение на субектите на данни, или когато основните дейности на администратора или на обработващия лични данни се състоят в мащабно обработване на специални категории лични данни и данни относно присъди и нарушения, администраторът или обработващият лични данни следва да бъде подпомаган при наблюдението на вътрешното спазване на настоящия регламент от лице с експертни познания в областта на правото и практиките за защита на данните. В частния сектор основните дейности на администратора се отнасят до неговите първични дейности, а не до обработването на лични данни като вторични дейности. Необходимото ниво на експертни познания следва да се определя по-специално в съответствие с извършваните операции по обработване на данни и защитата, която е необходима за личните данни, обработвани от администратора или обработващия лични данни. Тези служители по защита на данните, независимо от това дали са служители на администратора, следва да бъдат в състояние да изпълняват своите задължения и задачи независимо.

Член 37

Определяне на длъжностното лице по защита на данните

1. Администраторът и обработващият лични данни определят длъжностно лице по защита на данните във всички случаи, когато:

а) обработването се извършва от публичен орган или структура, освен когато става въпрос за съдилища при изпълнение на съдебните им функции;

б) основните дейности на администратора или обработващия лични данни се състоят в операции по обработване, които поради своето естество, обхват и/или

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

цели изискват редовно и систематично мащабно наблюдение на субектите на данни; или

в) основните дейности на администратора или обработващия лични данни се състоят в мащабно обработване на специалните категории данни съгласно член 9 и на лични данни, свързани с присъди и нарушения, по член 10.

2. Група предприятия може да назначи едно длъжностно лице по защита на данните, при условие че от всяко предприятие има лесен достъп до длъжностно лице по защита на данните.

3. Когато администраторът или обработващият лични данни е обществен орган или структура, едно длъжностно лице по защита на данните може да бъде назначено за няколко такива органа или структури, като се отчита организационната им структура и размер.

4. В случаи, различни от посочените в параграф 1, администраторът или обработващият лични данни или сдружения и други структури, представляващи категории администратори или обработващи лични данни, могат да определят — или ако това се иска от правото на Съюза или право на държава членка определят — длъжностно лице по защита на данните. Длъжностното лице по защита на данните може да действа в полза на такива сдружения и други структури, представляващи администратори или обработващи лични данни.

5. Длъжностното лице по защита на данните се определя въз основа на неговите професионални качества, и по-специално въз основа на експертните му познания в областта на законодателството и практиките в областта на защитата на данните и способността му да изпълнява задачите, посочени в член 39.

6. Длъжностното лице по защита на данните може да бъде член на персонала на администратора или на обработващия лични данни или да изпълнява задачите въз основа на договор за услуги.

7. Администраторът или обработващият лични данни публикува данните за контакт с длъжностното лице по защита на данните и ги съобщава на надзорния орган.

Член 38

Длъжност на длъжностното лице по защита на данните

1. Администраторът и обработващият лични данни гарантират, че длъжностното лице по защита на данните участва по подходящ начин и своевременно във всички въпроси, свързани със защитата на личните данни.

2. Администраторът и обработващият лични данни подпомагат длъжностното лице по защита на данните при изпълнението на посочените в член 39 задачи, като осигуряват ресурсите, необходими за изпълнението на тези задачи, и достъп до

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

личните данни и операциите по обработване, а така също поддържат неговите експертни знания.

3. Администраторът и обработващият лични данни правят необходимото длъжностното лице по защита на данните да не получава никакви указания във връзка с изпълнението на тези задачи. Длъжностното лице по защита на данните не може да бъде освобождавано от длъжност, нито санкционирано от администратора или обработващия лични данни за изпълнението на своите задачи. Длъжностното лице по защита на данните се отчита пряко пред най-висшето ръководно ниво на администратора или обработващия лични данни.

4. Субектите на данни могат да се обръщат към длъжностното лице по защита на данните по всички въпроси, свързани с обработването на техните лични данни и с упражняването на техните права съгласно настоящия регламент.

5. Длъжностното лице по защита на данните е длъжно да спазва секретността или поверителността на изпълняваните от него задачи в съответствие с правото на Съюза или правото на държава членка.

6. Длъжностното лице по защита на данните може да изпълнява и други задачи и задължения. Администраторът или обработващият лични данни прави необходимото тези задачи и задължения да не водят до конфликт на интереси.

Член 39

Задачи на длъжностното лице по защита на данните

1. Длъжностното лице по защита на данните изпълнява най-малко следните задачи:

а) да информира и съветва администратора или обработващия лични данни и служителите, които извършват обработване, за техните задължения по силата на настоящия регламент и на други разпоредби за защитата на данни на равнище Съюз или държава членка;

б) да наблюдава спазването на настоящия регламент и на други разпоредби за защитата на данни на равнище Съюз или държава членка и на политиките на администратора или обработващия лични данни по отношение на защитата на личните данни, включително възлагането на отговорности, повишаването на осведомеността и обучението на персонала, участващ в операциите по обработване, и съответните одити;

в) при поискване да предоставя съвети по отношение на оценката на въздействието върху защитата на данните и да наблюдава извършването на оценката съгласно член 35;

г) да си сътрудничи с надзорния орган;

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

д) да действа като точка за контакт за надзорния орган по въпроси, свързани с обработването, включително предварителната консултация, посочена в член 36, и по целесъобразност да се консултира по всякакви други въпроси.

2. При изпълнението на своите задачи длъжностното лице по защита на данните надлежно отчита рисковете, свързани с операциите по обработване, и се съобразява с естеството, обхвата, контекста и целите на обработката.

2. Назначаване на Длъжностно лице по защита на данните (ДЛЗД)

2.1. Задължително назначаване по GDPR

2.1.1. Публичен орган

GDPR не съдържа легална дефиниция на „публичен орган“. Дали дадено физическо или юридическо лице е публичен орган, се преценява според националното законодателство на държавата членка. Това понятие трябва да се тълкува **разширително** и при всички положения включва органи на национални, регионални и **местни власти**. Според Работната група по чл. 29, понятието публичен орган може да включва и физически/юридически лица, чиито дейности се регулират от публичното право (например публичен транспорт, електроснабдяване и водоснабдяване, транспортна инфраструктура, държавни медии, социално настаняване или дисциплинарни органи за контрол върху определена професия)[i]. Логиката, която стои зад това тълкуване е, че някои граждани (т. нар. субекти на данни от Регламента) имат ограничен избор дали и как ще се обработват личните им данни от подобни организации. Въпреки че подобно тълкуване на закона не е задължително или обвързващо, се препоръчва да му бъде обърнато специално внимание при анализа и преценката дали да се назначи ДЛЗД.

Трябва да се отбележи, че Работната група по чл. 29 препоръчва като добра практика да се назначи ДЛЗД, чиито функции да покриват и всички изпълнявани операции, включително тези, които не са свързани с упражняването на публичните функции (например отношенията със служителите на дадена община)[ii]. Никоя от разпоредбите на GDPR не изисква назначаване на ДЛЗД, чийто обхват на задължения включва единствено дейностите по обработването, свързани с публичните функции. Най-разумното и безопасно тълкуване е, че органите на местните власти трябва да назначат ДЛЗД, което да отговораря за всички дейности по обработване на данни в организацията (комуникация с граждани, служители, кандидати за работа, бивши служители, други публични власти и др.).

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

2.1.2. Основните дейности на администратора/ обработващия […] изискват редовно и систематично мащабно наблюдение на субектите

В общия случай, дейностите по обработване на данни от органите на местните власти би трябвало да попадат в обхвата на подточка 2.1.1 по-горе, тоест те трябва да назначат ДЛЗД въз основа на техния статут на публичен орган. За по-голяма яснота, по-долу следва кратък анализ на другите две хипотези по GDPR, чието наличие прави назначаването на ДЛЗД. Информацията може да е полезна за частни организации, чиито капитал е частично или изцяло притежаван от общината или друг орган на местните власти/ държавата и които не попадат в обхвата на терминан „публичен орган“.

Под термина **„основни дейности“** трябва да се разбират най-важните операции, нужни да се постигнат целите на администратора или на обработващия данните[iii]. Примерите, дадени от Работна група по чл. 29, включват обработването на здравни досиета в болници или наблюдение, осъществявано от частна компания. В същото време дейности по стандартната IT поддържка са изключени от „основните дейности“ на организацията[iv].

Понятието за **„голям мащаб“** не е специално дефинирано в GDPR. Споменава се изрично, че обработването на регионално, национално или наднационално ниво, която включва значително количество данни, и която би могла да засегне голям брой субекти и би могла да носи висок риск, може да се определи като обработване в „голям мащаб“.

Работната група по чл. 29 е предоставила примерен списък на дейностите, представляващи обработване в голям мащаб:

- обработване на данни на пациенти в болница;
- обработване на данни за пътувания на физически лица, използващи публичен транспорт (тоест проследяване на карти за пътувания);
- обработване на данни от гео-локация в реално време на клиенти на международна компания за бързо хранене за статистически цели от обработващ на данни, специализиран в подобни услуги;
- обработване на данни на клиенти от застрахователни компании/банки;
- обработване на лични данни от търсачка с цел поведенческа реклама;
- обработване на данни (съдържание, трафик, местоположение) от доставчици на телефонни и интернет услуги[v].

Понятието „обичаен“ е изначално свързано с обработване, което се извършва постоянно или периодично. Понятието „систематично наблюдение“ изисква обработването да се прави по определен план, стратегия или подобна предварително установена методология, по организиран начин, в система[vi].

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

Примери са управление на телекомуникационни мрежи, профилиране, поведенческа реклама, обработване на информация от smart устройства и др.

2.1.3. Основните дейности на администратора или на обработващия лични данни се състоят в мащабно обработване на специални категории лични данни и данни относно присъди и нарушения

След като термините „основни дейности“ и „голям мащаб“ бяха разгледани по-горе, в точка 2.1.2, настоящата точка ще обърне внимание на онова, което следва да се разбира под специални категории лични данни.

На първо място, съюзът „и“ трябва да се тълкува корективно като „или“. Казано по друг начин, всяко обработване, което включва **което и да е от двата вида обработване:** на специални категории данни или данни относно присъди и нарушения, когато то се извършва в голям мащаб и е част от основната дейност на организацията, изисква назначаването на ДЛЗД.

Специалните категории дата са:

- лични данни, разкриващи расов или етнически произход;
- политически мнения;
- религиозни или философски възгледи;
- членство в синдикални организации;
- генетични данни;
- биометрични данни за целите единствено на идентифицирането на физическо лице;
- данни за здравословното състояние или данни за сексуалния живот или сексуалната ориентация на физическото лице.

Категорията „личните данни, свързани с присъди и нарушения“, може да включва информация, съдържаща се в съдебни присъди, свидетелства за съдимост, актове на разследващи органи и др.

2.2. Други ситуации, в които се назначава ДЛЗД

2.2.1. Задължително назначаване по правото на ЕС/правото на държавата членка

Според чл. 37(4) GDPR, ЕС и/или държавите членки имат правото да определят и други хипотези, в които назначаването на ДЗЛД е задължително. Такова задължително назначаване може да произлиза от качествено изискване (например за типове обработване, които са специфични за определен сектор) или от количествено изискване (например ако организацията обработва данните на определен брой субекти). Германия например е въвела в националното си законодателство за защита на личните данни по-широки изисквания от GDPR:

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

- компании, извършващи стопанска дейност в Германия, и ангажиращи поне 10 човека в областта на автоматичното обработване ще са задължени да назначат ДЛЗД;
- в случаи на автоматично обработване при бизнес операции с цел трансфер, анонимизиран трансфер, или пазарно проучване и проучване на общественото мнение. Компаниите трябва да назначат ДЛЗД, независимо от броя служители, заети с автоматичното обработване на данни[vii].

2.2.2. Доброволно назначаване

GDPR също предвижда възможността ДЛЗД да се назначи доброволно. Подобен подход може да е разумен при организации, които искат да демонстрират, спазването на правилата за защита на личните данни и които искат да поощрят политиките на прозрачност и доверие. След като дейността на местните власти по-скоро би попаднала в първото задължително изискване (публичен орган), доброволното назначаване може да се приложи при определени организации, чийто капитал се притежава от общината/държавата – напр. публичен транспорт, общински училища/университети, обществени доставчици на услуги (електричество, вода) и други.

2.3. Договорни отношения с ДЛЗД

2.3.1. Трудов договор

GDPR изрично предвижда възможността да се назначи ДЛЗД на трудов договор. Това предполага две възможности: (i) да се назначи някой, който вече работи в организацията, и ще съчетава функциите си с тези на ДЛЗД, или (ii) да се разкрие нова работна позиция „ДЛЗД“. Изборът между тези две възможности зависи от структурата, броя на служителите, натовареността и вида и броя на дейностите по обработването и трябва да се направи на базата на конкретните обстоятелства. Ако съответният орган на местна власт е относително малък (например в кметство на малко населено място с ограничен брой жители, чиито данни се обработват), би било разумно да не се назначава нов служител, а функциите на ДЛЗД да се преразпределят към някой, вече работещ в организацията (като при всички случаи трябва да се избягва конфликт на интереси). Обратното, ако организацията на местна власт е сравнително голяма и/или ежедневните ѝ дейности са свързани с обработването на големи количества лични данни (или чувствителни данни/данни, свързани с присъди и нарушения), изборът да се открие позиция за ДЛЗД би бил оправдан.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

2.3.2. Договор за услуга

GDPR не задължава организациите да назначават ДЛЗД само на щат. Регламентът изрично предвижда и функциите на ДЛЗД да могат да се изпълняват от външни изпълнители (т. нар. outsourcing) на основата на договор за услуга. Работната група по чл. 29 препоръчва като добра практика външните екипи от ДЛЗД да имат посочен главен човек за контакт и служител, отговарящ за всеки клиент, което трябва да се уточни в договора за услуга[viii]. Освен това, всеки член на външната ДЛЗД организация трябва да отговаря на изискванията на GDPR.

Да се прехвърлят функциите на ДЛЗД на външна организация би било разумно, ако въпросната организация има нужното ниво на експертни познания, опит и притежава относими сертификати[ix].

Накрая, но не на последно място, по националното законодателство може да се налага да се извършат някои формални процедури, за да се сключи договор с външно ДЛЗД (например обществена поръчка).

3. ПОЗИЦИЯ НА ДЛЗД

3.1. Участие във всички въпроси, свързани със защитата на личните данни

GDPR изрично предвижда, че ДЛЗД трябва да участва във всички въпроси, свързани със защитата на личните данни в една организация. Работната група по чл. 29 препоръчва участието на ДЗЛД от най-ранния възможен етап (с консултации, съвети, контрол и т.н.) във всеки процес, включващ обработка на лични данни, като един от начините да се осигури защита на данните на етапа на проектирането[x].

Практически измерения от участието на ДЛЗД в организацията могат да са:

- даване на становище при извършването на оценка на въздействието върху защитата на лични данни; Чл. 35, пар. 2 от GDPR
- участие в работни срещи; Работната група по чл. 29 препоръчва участие в срещите на средно и високо равнище, но на практика отношенията на ДЛЗД с експертите би имал подобно (ако не и по-ефикасно) действие;
- консултиране всеки път, когато трябва да се вземе управленско решение относно защитата на лични данни;
- консултиране относно подходящи мерки, при случаи на нарушаване на сигурността на личните данни.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

3.2. Осигуряване на нужните ресурси и на независимост

ДЛЗД не може да изпълнява ефикасно длъжността си, ако не са му осигурени определени ресурси. Ръководството на организацията е отговорно да осигури на ДЛЗД ресурси поне по отношение на:

- **Организационни въпроси:**
  - ДЛЗД трябва да има екип, който да го подкрепи в изпълнението на задачите му. Това е от особена важност при големи организации. В някои случаи може да се наложи назначаването на няколко ДЛЗД;
  - достъп до всички други екипи в организацията. ДЛЗД не може да изпълнява функциите си ефикасно, ако не комуникира с всички други екипи, отговорни за обработването на лични данни (напр. регистратура, архив, правен отдел, човешки ресурси, счетоводство, IT отдел и др.);
  - отчитане само пред най-висшето ръководство. GDPR изрично предвижда, че ДЗЛД се отчита само пред висшето ръководство на организацията. За органите на местните власти това може да е кметът, общинският съвет, директорът/председателят на съответния административен отдел и т.н. Това изискване е много важно по отношение на осигуряване на независимостта на ДЗЛД. Ако връзката на ДЗЛД е индиректна (тоест чрез посредници като ръководителя на правния отдел или на отдел човешки ресурси), ДЛЗД не би могло да изпълнява функциите си ефикасно, защото би се отчитало на някой, върху когото трябва да упражнява контрол;
  - достатъчно време за изпълнение на функциите. Това изискване трябва специално да се спазва по отношение на ДЛЗД, което е наето на непълно работно време или при външно ДЛЗД, което има и други задължения, освен защитата на лични данни[xi]. Работната група по чл. 29 отбелязва като добра практика да се установи процент от времето за изпълнение на функцията по защита на личните данни, ако тя не се изпълнява на пълно работно време;
- **Финансови въпроси**
  - ДЛЗД трябва да разполага с нужните финансови ресурси, за да изпълнява функциите си. Ако организацията не осигурява достатъчно голям бюджет за дейности по защита на личните данни, ефикасното изпълнение на функциите на ДЛЗД може да бъде застрашено;
  - ДЛЗД трябва да има на разположение нужните помещения и оборудване (стаи, компютри, връзка с интернет, бази данни, технически решения като софтуерни програми и други);

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

- **Обучителни въпроси** – нивото на експертни познания на ДЛЗД трябва да бъде подобрявано постоянно (чрез курсове, осигуряване на нова литература и др). Като се има предвид, че защитата на личните данни е много динамична област на познанието, логично е ДЛЗД да трябва да е в крак с последните тенденции и подобрения, за да може да осигури най-високото ниво на защита на личните данни в организацията и да посрещне най-новите предизвикателства по отношение на технологичното и правното развитие.

Важен аспект от независимостта на ДЛЗД е забраната то да се санкционира и да понася неблагоприятни последици във връзка с изпълнението на функциите си. Тези неблагоприятни последици могат да варират - от уволнение или други видове дисциплинарни наказания до отказване на повишение, отказване на бонуси, давани на други служители, и др. Това, което може да се очаква от държавите членки, е да въведат промени в трудовото си законодателство и да осигурят защита на ДЛЗД срещу уволнение за периода на изпълнение на функциите им и известен период след това[xii]. В същото време, трябва да се направи едно важно уточнение за тази забрана – ДЛЗД не може да се санкционира за съвестното изпълнение на задълженията си. Но ако ДЛЗД не притежава нужните знания, умения, допуска дисциплинарни нарушения и др., организацията може да го уволни на всички основания, предвидени в националното трудово законодателство.

3.3. Конфликт на интереси

Ако ДЛЗД е назначено на трудов договор, това назначение не трябва да предизвиква конфликт на интереси. Конфликт на интереси би могъл да настъпи, ако ДЛЗД има друга функция в същата организация и определя целите и начините за обработване на данни в рамките на определени вътрешни процеси. Казано по друг начин, ДЛЗД не може да е също директор, изпълнителен директор, оперативен директор, финансов директор, ръководител на човешки ресурси или на IT отдел[xiii]. В допълнение, други роли, по-надолу в организационната структура, могат също да предизвикат конфликт на интереси, ако включват определяне на целите и начините на обработване (напр. счетоводител, юрисконсулт, IT специалист).

Конфликт на интереси може да произлезе не само при назначаване на ДЛЗД на трудов договор, но и при външно ДЛЗД. Ако ДЛЗД трябва да представлява администратор и обработващ данните пред съд по отношение на дело, засягащо защита на личните данни, ще се появи такъв конфликт, защото администраторът и обработващият ще имат противоположни интереси.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

4. ФУНКЦИИ НА ДЛЗД

4.1. Наблюдение

Една от ключовите функции на ДЛЗД е да наблюдава всички дейности по обработване на данни в организацията. Наблюдението е неразривно свързано с получаването, събирането на информация и правенето на уточнения, препоръки и становища в организацията. Функцията по наблюдение е с фокус върху вътрешните процеси в организацията, следователно информирани и консултирани трябва да са не само членовете на ръководството, но също и служителите на експертно ниво, чиито задължения са свързани с обработването на лични данни.

4.2. Оценка на въздействието върху защитата на лични данни (ОВЗЛД)

GDPR урежда участието на ДЛЗД в ОВЗЛД със съвещателни функции. Работната група по чл. 29 препоръчва като добра практика да се търси становище от ДЛЗД по отношение на един или повече от следните въпроси, свързани с оценката на въздействието:

- дали въобще да се прави ОВЗЛД;
- каква методология да се използва при извършването на ОВЗЛД;
- дали ОВЗЛД да се направи вътрешно или да се делегира на външен изпълнител;
- какви предпазни механизми (включително технически и организационни мерки) да се приложат, за да се намалят рисковете за правата и интересите на субектите на данни;
- дали ОВЗЛД е била извършена правилно и дали изводите от нея са в съответствие с GDPR[xiv].

Ако ръководството на организацията реши да се отклони от становището на ДЛЗД, добре е като част от принципа за отчетност това решение и причините за него да се документират и да могат да се представят на контролните органи в случай на проверка.

4.3. Точка за контакт

ДЛЗД е основната точка за контакт и за контролните органи (чл. 39, пар. 1, точка “е” от GDPR), и за лицата (субектите на данни) (чл. 38, пар. 4 от GDPR) по отношение на всякакви въпроси, свързани със защитата на лични данни в организацията. Следователно, от най-голяма важност е да се предаде информацията за връзка на ДЛЗД на контролния орган и на субектите на данни.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

Още повече, че изискването да се даде информация за контакт на ДЛЗД е един от елементите на принципа за прозрачност по чл. 12 GDPR.

Нищо в GDPR не забранява ДЛЗД да потърси становище от контролните органи по отношение на въпрос, свързан със защитата на личните данни в организацията.

4.4. Поддържане на регистри

Въпреки че задължението да се поддържат регистри е вменено на администраторите и на обработващите данни, а не на ДЛЗД, GDPR не забранява тази задача да се прехвърли на ДЛЗД. Функциите на ДЛЗД в GDPR са **минимален брой**, следователно организациите са свободни да им делегират други задачи. Работната група по чл. 29 счита, че да се прехвърли поддържането на регистри на ДЛЗД е един от начините да му се позволи да изпълнява функциите си по следене за спазването на регламента и по даване на информация и становища на администратора/обработващия данни[xv]. Тъй като регистрите са ефективен начин да се гарантира отчетност, би било разумно това задължение да се прехвърли на ДЛЗД.

5. ЗАКЛЮЧЕНИЕ И ПРАКТИЧЕСКИ СЪВЕТИ

ДЛЗД е една от основните фигури, гарантиращи спазването на новите правила за защита на личните данни. Важността на тази роля зависи от съответната организация. Ако организацията включи по правилен начин ДЛЗД във всички въпроси, свързани със защита на личните данни и му осигури ресурсите, нужни да си изпълнява функциите, ДЛЗД би могло да е един от ключовите фактори за осигуряването на съответствие с Регламента и за изграждането на доверие. В противен случай, ДЛЗД би било една изкуствена фигура без други истински функции, освен да движи комуникацията, свързана със защита на личните данни, което не е идеята на GDPR.

Органите на местните власти следва да се насърчават да назначат квалифицирани ДЛЗД, което може да бъде трудна задача, предвид липсата на подготвени експерти на европейско равнище. Във всеки случай, следващите няколко години ще определят как ще се развие ролята на ДЛЗД. Би било положително за обществото, ако именно органите на местните власти са едни от първите примери за това как най-добре да се използва фигурата на ДЛЗД.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

6. ВЪНШНИ ИЗТОЧНИЦИ И ЛИНКОВЕ

Книги

- **Harting, N.** Datenschutz-Grundverordnung: Das neue Datenschutzrecht in der betrieblichen Praxis, Verlag Dr. Otto Schmidt KG, Köln, 2016;
- **Voigt, P., von dem Bussche, A.** The EU General Data Protection Regulation (GDPR) – A Practical Guide, Springer International Publishing (2017);
- **Boardman, R., Mullock, J., Mole, A.** Bird & Bird Guide to General Data Protection Regulation (2016);
- **EU** General Data Protection Regulation (GDPR). An Implementation and Compliance Guide, IT Governance Publishing, Cambridgeshire (2016);

Документи на Работната група по чл. 29

- WP29, Guidelines on Data Protection Officers ('DPOs'), WP 243 rev.01;

Интернет връзки

- http://europa.eu/rapid/press-release_IP-18-386_en.htm
- https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en"

7. ПРЕПРАТКИ

[i] WP29, Guidelines on Data Protection Officers ('DPOs'), WP 243 rev.01, стр. 6.
[ii] Ibid.
[iii] Ibid.
[iv] Ibid, стр. 6-7.
[v] Ibid, стр. 8.
[vi] Вж точното тълкуване на РГ29 WP29 в WP29, Guidelines on Data Protection Officers ('DPOs'), WP 243 rev.01, стр. 8.
[vii] Demmel, A. The New German Federal Data Protection Act, Squire Patton Boggs, URL: <https://www.squirepattonboggs.com/~/media/files/insights/publications/2017/09/the-new-german-federal-data-protection-act/27836--german-federal-data-protection-alert.pdf> (26.03.2018);
[viii] WP29, Guidelines on Data Protection Officers ('DPOs'), WP 243 rev.01, стр. 22-23.
[ix] EU General Data Protection Regulation (GDPR). An Implementation and Compliance Guide, IT Governance Publishing, Cambridgeshire (2016), стр. 58.
[x] WP29, Guidelines on Data Protection Officers ('DPOs'), WP 243 rev.01, стр. 13.
[xi] Ibid, стр. 14.
[xii] Германия вече е въвела защита за ДЛЗД срещу уволнение 1 година, след като назначението е приключило, освен при извънредни причини за прекратяване на договора. Вж Demmel, A. The New German Federal Data Protection Act, Squire Patton Boggs, URL:

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

<https://www.squirepattonboggs.com/~/media/files/insights/publications/2017/09/the-new-german-federal-data-protection-act/27836--german-federal-data-protection-alert.pdf> (26.03.2018);

[xiii] WP29, Guidelines on Data Protection Officers ('DPOs'), WP 243 rev.01, стр. 16.

[xiv] Ibid, стр. 17.

[xv] WP29, Guidelines on Data Protection Officers ('DPOs'), WP 243 rev.01, стр. 19.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

ProLegis

Оценка на въздействието върху защитата на данните

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

ProLegis

Съдържание

1. Правна рамка 4

1.1. Общ регламент за защита на личните данни (GDPR) 4

2. Кога е необходима Оценка на въздействието върху защитата на личните данни (ОВЗД)? 7

2.1. Основни положения 7

2.2. Случаи, при които изготвянето на ОВЗД е задължително 7

2.2.1. Допълнителни съображения относно необходимостта от провеждане на ОВЗД 8

2.2.2. Провеждане на ОВЗД за няколко подобни процеса по обработване на данни 8

2.2.3. Положителни и отрицателни списъци относно хипотезите на провеждане на ОВЗД 9

2.3. Времеви график за изготвяне на ОВЗД 9

2.4. Преглед на ОВЗД 10

2.5. Предварителна консултация с надзорния орган съгласно член 36 от GDPR 10

3. Кой отговаря за извършването на ОВЗД? 11

3.1. Основни положения 11

3.2. Участие в ОВЗД 11

4. Как да се извърши ОВЗД? 12

4.1. Основни положения 12

4.2. Извършване на ОВЗД 12

4.3. Минимално съдържание на ОВЗД 13

4.4. Процесът на ОВЗД 14

4.5. Включване на субектите на данни или техни представители 15

4.6. Доклад за изготвянето на оценка на въздействието върху защитата на лични данни 16

5. Заключения и практически съвети 18

6. Външни източници и уеб връзки 19

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

Книги и статии 19
Документи на работната група по член 29 20
Интернет линкове 20

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

1. Правна рамка

1.1. Общ регламент за защита на личните данни (GDPR)

Член 35

Оценка на въздействието върху защитата на данните

1. Когато съществува вероятност определен вид обработване, по-специално при което се използват нови технологии, и предвид естеството, обхвата, контекста и целите на обработването, да породи висок риск за правата и свободите на физическите лица, преди да бъде извършено обработването, администраторът извършва оценка на въздействието на предвидените операции по обработването върху защитата на личните данни. В една оценка може да бъде разгледан набор от сходни операции по обработване, които представляват сходни високи рискове.

2. При извършването на оценка на въздействието върху защитата на данните администраторът иска становището на длъжностното лице по защита на данните, когато такова е определено.

3. Оценката на въздействието върху защитата на данните, посочена в параграф 1, се изисква по-специално в случай че:

а) систематична и подробна оценка на личните аспекти по отношение на физически лица, която се базира на автоматично обработване, включително. профилиране, и служи за основа на решения, които имат правни последици за физическото лице или по подобен начин сериозно засягат физическото лице;

б) мащабно обработване на специални категории данни, посочени в член 9, параграф 1 или на лични данни за присъди и нарушения по член 10; или

в) систематично мащабно наблюдение на публично достъпна зона.

4. Надзорният орган съставя и оповестява списък на видовете операции по обработване, за които се изисква оценка на въздействието върху защитата на данните съгласно параграф 1. Надзорният орган съобщава тези списъци на Комитета, посочен в член 68.

5. Надзорният орган може също да състави и оповести списък на видовете операции по обработване, за които не се изисква оценка на въздействието върху защитата на данните. Надзорният орган съобщава тези списъци на Комитета.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

6. Преди приемането на списъците, посочени в параграфи 4 и 5, компетентният надзорен орган прилага посочения в член 63 механизъм за съгласуваност, ако тези списъци включват дейности за обработване, свързани с предлагането на стоки или услуги на субекти на данни или с наблюдението на тяхното поведение в няколко държави членки или могат съществено да засегнат свободното движение на лични данни в рамките на Съюза.

7. Оценката съдържа най-малко:

а) системен опис на предвидените операции по обработване и целите на обработването, включително, ако е приложимо, преследвания от администратора законен интерес;

б) оценка на необходимостта и пропорционалността на операциите по обработване по отношение на целите;

в) оценка на рисковете за правата и свободите на субектите на данни, посочени в параграф 1; и

г) мерките, предвидени за справяне с рисковете, включително гаранциите, мерките за сигурност и механизмите за осигуряване на защитата на личните данни и за демонстриране на спазването на настоящия регламент, като се вземат предвид правата и законните интереси на субектите на данни и на други заинтересовани лица.

8. При оценката на въздействието на операциите по обработване, извършвани от администраторите и обработващите лични данни, надлежно се отчита и спазването от тяхна страна на одобрените кодекси за поведение, посочени в член 340 особено за целите на оценката на въздействието върху защитата на данните.

9. Когато е целесъобразно, администраторът се обръща към субектите на данните или техните представители за становище относно планираното обработване, без да се засяга защитата на търговските или обществените интереси или сигурността на операциите по обработване.

10. Когато обработването съгласно член 6, параграф 1, буква в) или д) има правно основание в правото на Съюза или в правото на държавата членка, под чиято юрисдикция е администраторът, и това право регулира конкретната операция по обработване или набор от такива операции, и вече е извършена оценка на въздействието върху защитата на личните данни като част от

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

общата оценка на въздействието в контекста на приемането на това правно основание, параграфи 1—7 не се прилагат, освен ако държавите членки не сметнат за необходимо да направят такава оценка преди започването на дейностите за обработване.

11. При необходимост администраторът прави преглед, за да прецени дали обработването е в съответствие с оценката на въздействието върху защитата на данни, най-малкото когато има промяна в риска, с който са свързани операциите по обработване.

Съображения от (89) до (96):

Чл. 35 GDPR е тясно свързан с чл. 24, 25 и 32. Основната разлика между чл. 32 и чл. 35 е, че чл. 32 (Сигурност на обработването) е насочен към рискове, свързани с неблагоприятни събития като атаки, докато Оценката на въздействието върху защитата на личните данни (ОВЗД), базирана на член 35, **се фокусира главно върху рисковете, възникващи от постоянната обработка на данни.**

ОВЗД е важен инструмент за постигането на адекватно ниво за защита на данните чрез технологични средства (защита на данните на етап проектиране), както е предвидено в член 25, параграф 1. И двете са базирани на принципа на предпазливостта, т.е. да се идентифицират рисковете във фазата на проектирането, като се разглеждат съответните противодействащи мерки, преди да бъдат въведени в експлоатация процеси по обработване на данни.

ОВЗД е инструмент за идентифициране и анализ на такива рискове. В случаите, когато ОВЗД не е задължителна, все пак се изисква анализ на свързаните с това рискове, за да се изпълнят адекватно изискванията на чл. 25 и чл. 32. И двете разпоредби изрично се позовават на правата и свободите на физическите лица. Дълбочината и необходимото документиране на анализа на риска, която трябва да се извърши, зависят от сложността и риска на конкретния процес по обработване на лични данни. Ето защо препоръчваме писмено документиране на извършения анализа на риска.

Прилагането на принципа за защита на данните на етап проектиране надхвърля предварително определените рискове в най-съвременния анализ на риска и включва решения, приети на по-късен етап ad hoc от разработчиците на системи (инженерни методи за осигуряване на неприкосновеността на личния живот) при прилагането на принципа за свеждане на данните до минимум.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

2. Кога е необходима Оценка на въздействието върху защитата на личните данни (ОВЗД)[i]?

2.1. Основни положения

ОВЗД трябва да се извърши преди започването на процеси по обработване на лични данни, които носят висок риск за правата и свободите на физическите лица.

По принцип ОВЗД трябва да се извърши при всяка форма на обработване на лични данни, освен ако не може да се определи a priori, че правата и свободите на физическите лица не са засегнати от конкретната операция.

За кой тип обработване на данни трябва да се приеме такъв риск, напр. хипотезите, посочени в чл. 35, параграф 3 или в съображение 91? Тук се акцентира върху използването на т.нар. нови технологии - неясна правна концепция, въведена с GDPR по отношение на ОВЗД. Оценката на риска не само трябва да отчита съществуващите рискове, но и вероятността от възникване на бъдещи събития, идентифициране в прогнозен анализ. Резултатите от проведената ОВЗД трябва да бъдат документирани.

Тълкуването на разпоредбата на чл. 35, пар.1, изр. последно, във връзка с съображение (92), предоставя важна информация относно необходимостта от извършване на ОВЗД: "при определени обстоятелства може да бъде разумно и рентабилно предметът на дадена оценка на въздействието върху защитата на данните да обхваща повече от един проект, например когато обществени органи или структури възнамеряват да създадат общо приложение или платформа за обработване на данни или когато няколко администратори планират внедряването на общо приложение или среда за обработване на данните в цял промишлен сектор или сегмент или за широко използвана хоризонтална дейност."

2.2. Случаи, при които изготвянето на ОВЗД е задължително

В чл. 35, пар. 3 са изброени хипотезите, при които провеждането на ОВЗД е задължително:

(a) систематична и подробна оценка на личните аспекти по отношение на физически лица, която се базира на автоматично обработване, включително. профилиране, и служи за основа на решения, които имат правни последици за физическото лице или по подобен начин сериозно засягат физическото лице;

(b) мащабно обработване на специални категории данни, посочени в член 9, параграф 1 или на лични данни за присъди и нарушения по член 10; или

(c) систематично мащабно наблюдение на публично достъпна зона.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

2.2.1. Допълнителни съображения относно необходимостта от провеждане на ОВЗД

В съображение 91 са изброени други хипотези, които налагат провеждането на ОВЗД:

Действия по обработване на лични данни:

i) които потенциално включват голям брой лица и/или висок риск и/или използване на широкомащабни действия по обработване в съответствие с най-съвременните технологии;
ii) които включват висок риск и затрудняват упражняването на правата на субектите на данни;
iii) когато целта е вземане на решения относно конкретни физически лица след систематична и обстойна оценка на личните аспекти, свързани с физически лица, въз основа на профилиране на тези данни или след обработване на специални категории лични данни, биометрични данни или данни за присъди и нарушения или свързани с това мерки за сигурност;
iv) които са свързани с висок риск, тъй като възпрепятстват субектите на данни да упражняват дадено право или да използват някоя услуга или договор;
v) които представляват висок риск, защото систематично се провеждат в голям мащаб.

2.2.2. Провеждане на ОВЗД за няколко подобни процеса по обработване на данни

Чл. 35, пар. 1 гласи, че извършването на единна ОВЗД за системи за обработка на данни със сходно ниво на риск е позволено. На първо място следва да се установи наличието на прилика между процесите за обработване на лични данни. При оценяването на подобна прилика трябва да се вземе предвид цялостната цел на обработването на данни във всеки отделен случай. Съображение (92) посочва, че при отчитане на разходите, ОВЗД може да има по-широк обхват, например да се извърши заедно от организации със сходен предмет на дейност или да обедини администратори от един и същ сектор с цел да се анализират конкретните среда и процеси по обработване с провеждането на единна ОВЗД.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

2.2.3. Положителни и отрицателни списъци относно хипотезите на провеждане на ОВЗД

Предполага се, че надзорните органи ще публикуват положителни / отрицателни списъци, които да насочат администраторите на лични данни, дали в конкретен случай се изисква провеждането на ОВЗД. Тези списъци следва да определят видовете действия по обработване, изискващи ОВЗД ("позитивни списъци") и случаите, при които не се изисква ОВЗД ("отрицателни списъци"). И двата списъка трябва да бъдат препратени от надзорния орган до Европейския комитет по защита на данните като част от регулаторната съгласуваност (член 35, параграф 4), за да се осигури по-добра хармонизация в целия ЕС.

Следва да се отбележи, че Работната група по чл. 29 препоръчва да се проведе ОВЗД и в случаите, когато изглежда неясно дали е необходима ОВЗД, за да се отговори на законовите изисквания за адекватно ниво на защита на личните данни.

2.3. Времеви график за изготвяне на ОВЗД

Моментът и методът за изготвяне на ОВЗД, трябва да бъдат определени от администратора. Предвидени са и санкции за неизпълнение задължението за изготвяне на ОВЗД. Препоръчително, подготовката за ОВЗД да започне в най-ранния възможен етап от даден проект. Всяка структурна единица от конкретна организация, участваща в обработването на данни, следва да се включи. Препоръчва се и провеждането на обучение за повишаване на информираността на служителите относно необходимостта от ОВЗД в рамките на организацията.

Вземането на мерки за свеждане на риска до минимум на ранен етап при всеки проект, включващ обработване на данни, може да помогне за свеждане на бюрократичните усилия до разумно ниско ниво.

Резултатите от проведена ОВЗД могат да дадат насоки при търсенето на адекватни решения и да спомогнат ефективното и своевременно изпълнение на посочените по-горе изисквания за защита на данните чрез подходящи технически мерки (защита на данните на етап на проектиране) и избора на настройки по подразбиране, имащи отношение към защитата на данните.

Предоставяйки всеобхватна и интензивна подготовка, ОВЗД ще навигира изпълнението на даден планиран проект от концептуалния етап до окончателното му оперативно изпълнение и демонстрира итеративния характер на процеса по извършване на ОВЗД.

Дали изготвянето на ОВЗД е необходимо спрямо дейности по обработване, които се осъществяват преди началото на общата приложимост на GDPR (25 май

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

2018 г.), е отворен въпрос. Буквалното тълкуване на разпоредбата ("преди") сочи, че провеждането на ОВЗД се изисква само за процеси, чието изпълнение започва след 25 май 2018 г. или преминават през значителни промени след тази дата.

Тъй като в тези случаи дейностите по обработване на данни вече се случват, предварителна проверка не е възможна. Освен това тези дейности не съществуват в нерегламентирано пространство (при положение, че са взети под внимание всички правни разпоредби и изискванията за докладване по предходната правна рамка).

Въпреки това Работна група по член 29 силно препоръчва да се извърши ОВЗД на вече използваните системи за обработване, за да се избегнат правната несигурност и възможни санкции.

2.4. Преглед на ОВЗД

След извършването на ОВЗД изпълнението на предложените мерки трябва да бъде преразгледано, ако се сметне за необходимо, може да се наложи обследване на процеса по обработване на данните, за да се идентифицират новите рискови елементи. В съображение (89) се посочва, че може да е необходим повторен преглед на ОВЗД своевременно след първата оценка. При извършване на ОВЗД времевата рамка за рутинни проверки или бъдещи подновявания трябва да бъде включена като част от документацията.

Трябва да се вземат предвид технологичното развитие, нова правна уредба и промени в действията по обработване. Ако възникне възможност за рискова ситуация, следва да се извърши нова ОВЗД.

Задължението за извършване на ОВЗД е част от отговорностите на администратора на данни, отразяваща неговото съответствие с принципа на отчетност. Документацията и докладът трябва не само да предоставят информация за извършената ОВЗД, но и да изброяват всички причини, поради които не може да бъде направена пълна ОВЗД или за прекратяване на ОВЗД, идентифицирането на високи рискове за субектите на данни.

2.5. Предварителна консултация с надзорния орган съгласно член 36 от GDPR

Администраторът на лични данни се консултира с надзорния орган преди началото на даден процес по обработване, когато изготвената съгласно член 35 ОВЗД покаже, че обработването ще породи висок риск администраторът не знае какво мерки да предприеме за ограничаване на риска. Надзорният орган трябва да отговори на това искане за консултация в рамките на четиринадесет седмици. За сложни и иновативни проекти се препоръчва да се започне ОВЗД в най-ранния

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

възможен етап, така че всяка препоръка от надзорния орган може да бъде разгледана при изпълнението на плана на проекта.

3. Кой отговаря за извършването на ОВЗД?

3.1. Основни положения

Отговорността за провеждането на ОВЗД е на администратора - в случая, местните власти. Първоначално, в своето предложението Комисията поверява отговорността за провеждане на ОВЗД на обработващия данните, който действа по заповед на администратора. За разлика от това, приетия текст на регламента, в съображение (95) посочва единствено, че обработващият следва да съдейства на администратора, когато е необходимо и ако е изрично поискано, за да се осигури спазването на задълженията, произтичащи от ОВЗД.

Следователно, на практика е препоръчително при уреждане на отношенията между администратор и обработващ в договора да се съдържа задължения на обработващия да се включва и активно да подпомага целия процес по изготвяне на ОВЗД. Установяването на подобно задължение е извън обхвата на чл. 28, параграф 3, буква е, който предвижда, че договорът между администратор и обработващ (или всеки друг правен инструмент), която разпоредба определя че обработващият следва да взима предвид естеството на обработването и информацията, която е предоставена, за да гарантира съответствие със задълженията, произтичащи от чл. 32-36. Често само обработващият ще разполага с необходимата информация за оценка на съответните аспекти от даден процес по обработване на данни. При това положение трябва да се вземе предвид риска от разкриване на търговски тайна. Отново се препоръчва този въпрос да бъде уреден в договора между администратора и обработващия. Ако се предвижда обработване на данни от съвместни администратори, ОВЗД по смисъла на чл. 35, ал. 1, т. 2 може да се извърши и от единия от тях - което не освобождава другите от отговорност.

3.2. Участие в ОВЗД

Препоръчително е ОВЗД да бъде организирана като проект, със съответното разпределение на необходимите материални и човешки ресурси от ръководния екип на дадена организация. При съставянето на екипа на проекта трябва да се обърне особено внимание на сложността на проекта, необходимите специализирани знания и необходимите знания за конкретния проект и неговата среда. На практика може да се събере екип от юристи, IT персонал, CISO, длъжностно лице по защита на данните, отделът, който извършва конкретната дейност по обработване („собственикът“ на данните) и др.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

Особено внимание следа да се отдели на избягването на конфликт на интереси. Следователно, лицата, в бъдещи ще се занимават с обработването на данни, не трябва да се считат за независими, но от друга страна, могат да осигурят ценен принос към процеса на изготвяне на ОВЗД. Изпълнението може да се извърши от вътрешен екип, както и от външни трети лица. В идеалния случай трябва да бъде включен независим орган.

Администраторът следва да осигури участието на длъжностното лице по защита на данните в ОВЗД. Съгласно член 39, параграф 1, буква в) една от функциите на длъжностното лице по защита на данните е да дава консултации относно ОВЗД и да наблюдава нейното извършване, но само при поискване и не във водеща позиция.

Следователно, на лице е задължение на администратора да получи съвет от лицето по защита на данните. Кога и до каква степен лицето по защита на данните трябва да бъде включено в процеса, е решение на администратора. Например, преглед на окончателния доклад на изготвена на ОВЗД от негова страна също би било достатъчно. На практика, своевременното включване на длъжностното лице по защита на личните данни е силно препоръчително предвид специфичните му задачи и професионална подготовка.

В зависимост от вида на организацията и структурата на администратора, се препоръчва ОВЗД да се извършва след одобрение от ръководството или от съответния упълномощен орган.

4. Как да се извърши ОВЗД?

4.1. Основни положения

Тук следва да се отбележи, че GDPR не предвижда никаква конкретна форма или конкретен метод за изготвяне на ОВЗД – обект на дискусия на национално и европейско равнище. Работната група по член 29 отбелязва, че различни варианти за планиране на ОВЗД могат да бъдат използвани с оглед практическото прилагане на разпоредбите на GDPR и дава примери за съществуващи (общи или специфични за даден сектор) модели на план за ОВЗД в Приложение 1.[ii]

4.2. Извършване на ОВЗД

Предвид казаното по-горе, администраторът е свободен как да организира процеса по извършване на ОВЗД и може да го адаптира към съществуващите вътрешни процедури, стига органът на местната власт да вземе предвид четирите изисквания, съдържащи се в член 35, пар. 7 б. а) до г) от GDPR като минимални изисквания за ОВЗД, които Работната група по член 29 конкретизира. В

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

допълнение, администраторът следва да вземе под внимание включването на „заинтересовани страни" (вж. член 35, пар. 2) и гледната точка на субектите на данни (вж. 35, пар. 9):

а) системен опис на предвидените операции по обработване и целите на обработването, включително, ако е приложимо, преследвания от администратора законен интерес;

б) оценка на необходимостта и пропорционалността на операциите по обработване по отношение на целите;

в) оценка на рисковете за правата и свободите на субектите на данни, посочени в параграф 1; и

г) мерките, предвидени за справяне с рисковете, включително гаранциите, мерките за сигурност и механизмите за осигуряване на защитата на личните данни и за демонстриране на спазването на настоящия регламент, като се вземат предвид правата и законните интереси на субектите на данни и на други заинтересовани лица.

4.3. Минимално съдържание на ОВЗД

Член 35, пар. 7, букви от а) до г) в GDPR във връзка с съображения (84) и (90) се изисква най-малко:

i) Систематично описание на обекта на ОРЗД („обект на оценка“ в контекста на целия бизнес процес, не само действията по обработване на лични данни) и целта на обработването;

ii) Оценка за пропорционалността на обработването; в нейните рамки се определя дали планираният процес по обработване отговаря на изискванията за необходимост и пропорционалност с оглед на планираната цел на обработване.

iii) Оценка на риска, която се състои от три стъпки:

   i. Идентифициране на риск;

   ii. Анализ на риска (качествена класификация според сериозността на риска и възможността за неговото възникване);

   iii. Оценка на риска (напр. чрез рискова матрица);

iv) Третиране на риска (предприемане на мерки за управление на риска).

Точки iii) и iv) са проявления на т.нар. "подход, базиран на риска" на GDPR и са от значение не само при изготвянето на ОВЗД, но и при практическото приложение на чл. 24, 25 и 32 от GDPR. С други думи, ОВЗД е конкретен пример за подход при обработване на данни, основа на риска. Накратко, отнасящ се до данни, за които се очаква да доведат до висок риск за правата и свободите на физически лица и които изискват по-задълбочена обработка и оценка на риска. По принцип обаче всяка друга проверка за допустимост за обработване на данните е също присъща

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

на такава оценка на риска, включваща подходящи технически и организационни мерки, които намаляват риска, преди да бъдат приложени (вж. само член 24, параграф 1 от GDPR).

4.4. Процесът на ОВЗД

ОВЗД трябва да се разглежда като процес (а не само доклад), който трябва да започне възможно най-скоро, за да повлияе върху планирането на елементите на процеса по обработване на лични данни. В резултат на това, оценката на въздействието също се различава от одита, който оценява даден текущ процес по обработване и обикновено е твърде късно, за да "внедри" изискванията за защита на личните данни, които от своя ОВЗД формулира.

Понастоящем съществуват многобройни предложения за осъществяване на ОВЗД, който по един или друг начин е сходен с резултатите от проучването на PIAF (2012 г.) [iii], в което са описани методологии за оценка на въздействието върху неприкосновеността на личния живот в седем държави (вкл. извличане на препоръки за "най-добри практики" и основни елементи на процеса за оценка на въздействието върху неприкосновеността на личния живот). Идентифицирани са следните основни елементи:

- определяне дали оценка за въздействието върху неприкосновеността на личния живот (Privacy Impact Assessment) е необходима;
- определяне на екипа, отговорен за изготвяне на оценката и задачите му.
- описание на предложения проект [и определяне на заинтересованите страни];
- анализ на информационните потоци и други въздействия върху неприкосновеността на личния живот;
- консултация със заинтересованите страни;
- управление на риска [идентифициране на рисковете и възможните решения];
- проверка за законосъобразност;
- формулиране на препоръки;
- подготовка и публикуване на доклада [напр. на уебсайта на организацията];
- изпълнение на препоръките;
- външен преглед и / или одит [извършен от трети страни];
- преразглеждане на оценката, ако въпросния е в процес по обработване на лични данни е обект на промяна [актуализиране на Оценката, ако има кардинална промяна в процеса по обработване на лични данни].

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

Моделът на ОВЗД за интелигентни мрежи и интелигентни измервателни системи, който е изрично посочен в Препоръка 2014/724 / ЕС на Европейската комисия, предвижда следните стъпки:[iv]

- Стъпка 1: Предварителна оценка и определяне на критерии относно необходимостта от провеждане на ОВЗД.
- Стъпка 2: Инициириране.
- Стъпка 3: Идентификация, характеризиране и описание на интелигентни мрежови системи / приложения, обработващи лични данни.
- Стъпка 4: Идентифициране на съответните рискове.
- Стъпка 5: Оценка на риска за защита на данните.
- Стъпка 6: Идентификация и препоръка за контрол и остатъчни рискове.
- Стъпка 7: Документиране и изготвяне на доклад за ОВЗД.
- Стъпка 8: Преглед и поддръжка.

Новият стандарт ISO / IEC 29134 предоставя указания за процес за извършване на оценки на въздействието върху неприкосновеността на личния живот и за структурата и съдържанието на доклада на оценката. Процесът е разделен на следните четири подпроцеса:

- анализ на праговете.
- подготовка на оценка за въздействието върху неприкосновеността на личния живот.
- извършване на оценката.
- проследяване.

Как и на колко етапа е разделен процесът на ОВЗД, е по-скоро въпрос на разбиране, различни подходи варират например от три или четири фази, до над шест до седем етапа. По-скоро, това, което е важно, е разбираемата организация на процеса по изготвяне на ОВЗД, която отчита изискванията на чл. 35, пар. 7 GDPR и препоръките на Работната група по член 29.

4.5. Включване на субектите на данни или техни представители

Съгласно член 35, пар. 9, когато е целесъобразно, администраторът се обръща към субектите на данните или техни представители за становище относно планиран процес по обработване, без да се засяга защитата на търговските или обществените интереси или сигурността на операциите по обработване. В контекста на тристранните преговори не става ясно при какви обстоятелства би било „целесъобразно“ да се поиска становище на съответното лице или негов представител, както и в кои случаи е допустимо това не е необходимо.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

Начинът, по който се изисква становището, трябва да бъде съобразен с конкретиката на съответния процес по обработване. Работната група по чл. 29 признава различни форми за това, като провеждане на проучване (вътрешно или външно), официални интервюта с представители на персонала или синдикати и подаване на въпросник на бъдещи клиенти на администратора. Администраторът ще трябва да проучи възгледите на субектите на данни или техните представители и ще трябва да ги разгледа в рамките на изготвяне на ОРЗД. В доктрината има противоречиви гледни точки дали асоциациите за защита на потребителите могат да се включат в термина "представител".[v]

Във всеки случай, задължението за консултация изрично не се отнася до защитата на търговските или обществените интереси или безопасността на операциите по обработване. Поради това администраторът може да ограничи или да откаже в крайна сметка да изпълни задължението да предостави на засегнатите лица или на техните представители, информация относно планираното действие по обработване по член 35, пар. 9 (което в последния случай ще доведе до факта, че активно участие по смисъла на член 35, пар. 9 няма да бъде възможно, тъй като предоставянето на достатъчно информация е задължително условие за събиране на становището на засегнатите лица или на техните представители).

В рамките на изготвянето на ОРЗД, с оглед съблюдаването на принципа на отчетност, се препоръчва отразяването в доклада на ОРЗД защо са получени малко или изобщо не са били проучени становищата на засегнатите лица и техните представители и защо не са взети частично или изцяло под внимание в нейните резултати.

4.6. Доклад за изготвянето на оценка на въздействието върху защитата на лични данни

Трябва да се отбележи, че докладът за ОВЗД не е целта на ОВЗД, а "средство за довеждане до край" на документирането на процеса (вътрешен и външен). Отчитането не трябва да се подценява – то документира изпълнението и резултатите, а изготвянето на просто един PR доклад трябва да се избягва, тъй като със сигурно няма да отговори за изискванията за съответствие. Самият доклад може също така да служи като наръчник и контролен списък при провеждането на ОВЗД.

Член 35 на Регламента не съдържа, донякъде изненадващо, изрично изискване за изготвяне на доклад за провеждането на ОВЗД. Налице е обаче задължение за документиране от страна на администратора, което е безспорно и се извежда имплицитно от нормата член 35, пар. 7 от GDPR, както и от член 5, пар. 2 от GDPR (отчетност) във връзка с член 24, пар. 1 от GDPR и член 36, пар. 3, б. д

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

(което изисква от администратора да предостави "оценката на въздействието за защита на данните, посочена в член 35"). Също така преразглеждането, съгласно член 35, пар. 11, за да се прецени дали обработването на лични данни се извършва в съответствие с ОВЗД, изисква резултатите от оценката на въздействието да бъдат съхранени. Освен това докладването за извършените оценки на въздействието е в съответствие с глобалните практики в тази област (вж. Раздел IV.1 по-долу), което е в съответствието с нормата на чл. 35 GDPR.

Препоръчително е процесът на ОВЗД да е придружен с документация, в смисъла на "непрекъснато развиваща се документация", като се започне с документацията за анализа на праговете, в случай, че не е необходимо извършването на ОВЗД. Дори ако този анализ покаже, че не се изисква ОВЗД и процесът е прекратен, администраторът продължава да бъде отговорен за неговата отчетност. Тази писмена документация може да бъде представена на надзорния орган във всеки бъдещ процес, като по този начин се осигурява проследяване на за вътрешните съображения и оценки .

По отношение на съдържанието, докладът по същество следва да определи процедурата (включително представяне на фактите, в смисъл на систематично описание на целия предмет на теста - "цел на оценката") и резултатите от изготвянето на ОВЗД. Както в случая на самия процес на ОВЗД, GDPR не предвижда никакви специфични правила за изготвянето на доклад за ОВЗД. Въпреки това като минимално съдържание може да се препоръча включването на критериите, изброени от Работната група по член 29 в Приложение 2 към WP 248, които по същество се основават на член 35, параграф 7. ISO / IEC 29134 препоръчва следното съдържание на доклада за оценка на въздействието върху неприкосновеността на личния живот с акцент върху оценката на риска:

- релевантни изисквания за поверителност;
- описание на обхвата;
- описание на използваните критерии за определяне на риска;
- участници в изпълнението.
- консултации със заинтересованите страни.

Това се подкрепя и от съображение (90), в което се посочва, inter alia, както следва: *"оценката на въздействието следва да включва по-специално мерките, гаранциите и механизмите,предвидени за смекчаване на този риск, гарантиране на защитата на личните данни и доказване на спазването на настоящия регламент."*

В подробното проучване на PIAF, препоръчаното минималното съдържание на доклада за оценка на въздействието е, както следва:[vi]

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

- въведение и обща информация, включително кой е извършил оценката, координати за контакт и къде да се намери допълнителна информация и други източници за помощ и съвет;
- описание на проекта, на информационните потоци и на въздействието върху неприкосновеността на личния живот.
- резултати от консултациите със заинтересованите страни.
- описание на фазите за оценка на риска и за смекчаване на риска, включително разглежданите алтернативи.
- анализ на законосъобразността.
- препоръки.
- приложения, ако е необходимо.

Ако е налице отчет или последната версия на черновата, може да възникне въпросът какво трябва да се случи с отговорното лице, преди всичко дали и от кого трябва да бъде "одобрен" - практически релевантна точка, която не е уредена в GDPR. Службата на комисаря по информационните въпроси на Обединеното кралство (Information Commissioner's Office) изрично установява в своя Практически кодекс следното: "да има подходящо писмено становище в рамките на организацията". Ръководният орган обикновено взима финалното решение относно предмета и естеството на проекта за изготвяне на ОВЗД. Като минимален стандарт, ръководителят на проекта или длъжностното лице по защита на данните трябва да докладват на "най-високото управленско ниво", както е предвидено в чл. 38 (3) GDPR.

GDPR не предвижда задължение да публикуване на ОВЗД, но Работна група по член 29 препоръчва публикуването му (поне отчасти), с оглед повишаването на доверието в даден процес по обработване на лични насърчаването на прозрачността. По-специално, публикуването се насърчава в случаите, когато част от обществото ще бъде засегната от (планираната) дейност по обработване.

5. Заключения и практически съвети

През годините, регулаторите, разполагащи с достатъчно ресурси са разработили свои собствени подходи за оценка на въздействието върху неприкосновеността на личния живот. От днешна гледна точка, трябва да се очаква, че тези надзорни органи, които вече са разработили свой собствен модел, ще го предпочетат или ще го разпространяват, защото техните собствени препоръки ще бъдат най-силно изразени. Съдържанието на наличните понастоящем подходи за ОВЗД на националните надзорни органи (от държави-членки на ЕС) обикновено

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

предхождат GDPR и непоследователно (все още) се адаптира към изискванията или терминологията на GDPR.

ICO (великобританският надзорен орган) например добави изискванията и терминологията на GDPR към своя Практически кодекс за осъществяване на оценка на въздействието (PIA) (2014 г.) към доклада "Big data, artificial intelligence, machine learning and data protection"[vii]. Нещо, което се очаква и от други надзорни органи. Остава да се види дали Европейският комитет по защита на данните ще предостави насоки, препоръки и / или добри практики за ОВЗД в съответствие с чл. 70, пар. 1, б. д).

Препоръки накратко:

- документиране на всички решения, по-специално защо не е извършена ОВЗД (ако е приложимо);
- ако има съмнения, да се извърши ОВЗД;
- участие на вътрешни и външни заинтересувани лица;
- използване на подходи, добри практики и ако е уместно, подобни ОВЗД, които вече са налице
- Публикуване на ОВЗД:
  - Особено от публичните органи;
  - Повишава осведомеността за поверителността и изгражда доверие;

6. Външни източници и уеб връзки

Книги и статии

- ***Kastelitz, M., Hötzendorfer, W., Riedl, R***., Ausgewählte Fragen der Durchführung einer Datenschutz-Folgenabschätzung gemäß Art 35 DSGVO, Jahrbuch Datenschutzrecht 2017
- ***De Hert, Paul/Kloza, Dariusz/Wright, David,*** Recommendations for a privacy impact assessment framework for the European Union http://www.piafproject.eu/ref/PIAF_D3_final.pdf
- ***Wright, David/De Hert, Paul* (Ed.),** Privacy Impact Assessment, Springer Science & Business Media, Dordrecht, Heidelberg, London, New York 2012
- ***De Hert/Kloza/Wright*** (Ed.), **PIAF**, Recommendations for a privacy impact assessment framework for the European Union, Deliverable D3 (2012), http://piafproject.eu/ref/PIAF_D3_final.pdf; more available at http://piafproject.eu/Deliverables.html.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

- ***Martini in Paal/Pauly*** (Ed.), Datenschutz-Grundverordnung (2016) Art 35,; dagegen (mangels rechtlicher Verbundenheit) Laue/Nink/Kremer, Das neue Datenschutzrecht in der betrieblichen Praxis (2016) 245,

Документи на работната група по член 29

- Работна група по чл. 29, WP 248, April 4, 2017: Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679 http://ec.europa.eu/newsroom/document.cfm?doc_id=44137
- Работна група по чл. 29, WP 248, as last Revised and adopted on 4 October 2017 (rev.01): Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679 https://www.dsb.gv.at/documents/22758/112500/Guidelines_on_Data_Protection_Impact_Assessment_(DPIA).pdf/ed5daa8c-d388-43a6-9842-629b8175a99c

Интернет линкове

- Brussels Laboratory for Data Protection and Privacy Impact Assessments http://www.vub.ac.be/LSTS/dpialab/
- ICO, Big data, artificial intelligence, machine learning and data protection (2017), 99 f, https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf.

7. Препратки

[i] Настоящият раздел е силно повлиян от Kastelitz, M., Hötzendorfer, W., Riedl, R., Ausgewählte Fragen der Durchführung einer Datenschutz-Folgenabschätzung gemäß Art 35 DSGVO, Jahrbuch Datenschutzrecht 2017, 113ff.

ii Работна група по чл. 29, WP 248, 15: Могат да се използват различни методологии (вж. Приложение 1 на документа за примери на методологии за изготвяне на ОВЗД), при изпълнението на изискванията, заложени в GDPR.

[iii] *De Hert/Kloza/Wright* (Hrsg), PIAF, Recommendations for a privacy impact assessment framework for the European Union, Deliverable D3 (2012), http://piafproject.eu/ref/PIAF_D3_final.pdf; more available at http://piafproject.eu/Deliverables.html.

iv Препоръка на Европейската комисия 2014/724/EU of 10 октомври 2014 on the Data Protection Impact Assessment Template for Smart Grid and Smart Metering Systems, ABl L 2014/300, стр. 63.

v *Martini* in Paal/Pauly (Hrsg), Datenschutz-Grundverordnung (2016) Art 35 Rz 60; dagegen (mangels rechtlicher Verbundenheit) *Laue/Nink/Kremer*, Das neue Datenschutzrecht in der betrieblichen Praxis (2016) 245 Rz 99.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

vi *De Hert/Kloza/Wright* (Hrsg), PIAF, Recommendations for a privacy impact assessment framework for the European Union, Deliverable D3 (2012) 31, http://piafproject.eu/ref/PIAF_D3_final.pdf.

vii ICO, Big data, artificial intelligence, machine learning and data protection (2017), 99 f, https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

ProLegis

ПРОЗРАЧНОСТ

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

ProLegis

СЪДЪРЖАНИЕ

1. ПРАВНА РАМКА 4
   1.1. Договори на Европейския съюз 4
   1.2. Харта на основните права на ЕС 4
   1.3. Общ регламент за защита на данните (GDPR) 4
2. ЗНАЧЕНИЕ НА ПРИНЦИПА НА ПРОЗРАЧНОСТ В GDPR 6
   2.1. Елементи на прозрачността в GDPR (чл. 12) 6
      2.1.1. “Кратка, прозрачна, разбираема и леснодостъпна форма” 6
      2.1.2. “Ясен и прост език” 7
      2.1.3. Начин на представяне на информацията (Чл. 12, пар. 1 и пар. 5 “безплатно”) 7
   2.2. Информация, която трябва да се предостави на субектите (Чл. 13 и 14) ... 7
      2.2.1. Каква информация трябва да се предостави? 7
      2.2.2. Каква допълнителна информация трябва да се предостави? 8
      2.2.3 Как трябва да се предостави информацията? 9
      2.2.4 Кога се предоставя информация? 9
      2.2.5. Кога да се предостави съобщение в случай на промени в информацията по прозрачността, която администраторите трябва да предоставят? 10
   2.3. Условия 10
      2.3.1. Съобщения относно нивото на защита на личните данни 10
      2.3.2. “Push” & “pull” уведомления 10
      2.3.3. Други видове „подходящи мерки“ 11
      2.3.4. Визуализация 11
   2.4. Упражняване правата на гражданите 12
      2.4.1. Изключения от задължението да се предостави информация 12
3. ЗАКЛЮЧЕНИЕ И ПРАКТИЧЕСКИ СЪВЕТИ 13

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

4. ВЪНШНИ ИЗТОЧНИЦИ И ЛИНКОВЕ 14
Книги 14
Документи на Работната група по чл. 29 14
Онлайн връзки 14
5. ПРЕПРАТКИ 14

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

1. ПРАВНА РАМКА

1.1. Договори на Европейския съюз

Член 1 от ДЕС -> Решенията се вземат „при възможно най-голямо зачитане на принципа на откритост и възможно най-близко до гражданите."

Член 11, параграф 2 от ДЕС -> "Институциите поддържат открит, прозрачен и редовен диалог с представителните организации и гражданското общество."

Член 15, параграф 3 от ДФЕС - Всеки гражданин на Съюза има право на достъп до документите на институциите, органите, службите и агенциите на Съюза, независимо от вида на техния носител, при спазване на принципите и условията, които следва да бъдат определени в съответствие с настоящия параграф.

1.2. Харта на основните права на ЕС

Прозрачността е ключов елемент от принципа за добросъвестно обработване на личните данни. Като такъв, тя е уредена в чл. 8 от Хартата на основните права на ЕС.

Член 8

Защита на личните данни

1. Всеки има право на защита на неговите лични данни.

2. Тези данни трябва да бъдат обработвани добросъвестно, за точно определени цели и въз основа на съгласието на заинтересованото лице или по силата на друго предвидено от закона легитимно основание. Всеки има право на достъп до събраните данни, отнасящи се до него, както и правото да изиска поправянето им.

3. Спазването на тези правила подлежи на контрол от независим орган.

1.3. Общ регламент за защита на данните (GDPR)

Съображение (39)

„Всяко обработване на лични данни следва да бъде законосъобразно и добросъвестно. За физическите лица следва да е прозрачно по какъв начин отнасящи се до тях лични данни се събират, използват, консултират или обработват по друг начин, както и в какъв обхват се извършва или ще се извършва обработването на данните. Принципът на прозрачност изисква всяка

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

информация и комуникация във връзка с обработването на тези лични данни да бъде лесно достъпна и разбираема и да се използват ясни и недвусмислени формулировки. Този принципа се отнася в особена степен за информацията, която получават субектите на данни за самоличността на администратора и целите на обработването, и за допълнителната информация, гарантираща добросъвестно и прозрачно обработване на данните по отношение на засегнатите физически лица и тяхното право да получат потвърждение и уведомление за съдържанието на свързани с тях лични данни, които се обработват. Физическите лица следва да бъдат информирани за рисковете, правилата, гаранциите и правата, свързани с обработването на лични данни, и за начините, по които да упражняват правата си по отношение на обработването…“

Съображение (58)

Принципът на прозрачност изисква всяка информация както за обществеността, така и за субекта на данните да бъде в кратка, прозрачна, разбираема и лесно достъпна форма и да се използват ясни и недвусмислени формулировки, а в допълнение когато е необходимо, да се използва и визуализация. Тази информация може да бъде представена в електронна форма, например чрез уебсайт, когато е адресирана до обществеността. Това важи в особена степен за ситуации, където нарастването на участниците и технологичната сложност на тази практика правят трудно за субекта на данни да узнае и разбере дали се събират свързани с него лични данни, от кого и с каква цел, като в случая на онлайн рекламите. Като се има предвид, че на децата се полага специална защита, когато обработването е насочено към дете, всяка информация и комуникация следва да се предоставя с ясни и недвусмислени формулировки, които да бъдат лесноразбираеми за детето.

Член 5, параграф 1

Принципи, свързани с обработването на лични данни

1. Личните данни са:

а) обработвани законосъобразно, добросъвестно и по прозрачен начин по отношение на субекта на данните („законосъобразност, добросъвестност и прозрачност“).

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

2. ЗНАЧЕНИЕ НА ПРИНЦИПА НА ПРОЗРАЧНОСТ В GDPR

Принципът на прозрачност е свързан с принципите на справедливост и отчетност. Член 5 (Принципи, свързани с обработването на лични данни) задължава администраторите да докажат, че личните данни се обработват по прозрачен начин. Според препоръките на Работната група по чл. 29[i], целта на принципа е да оправомощи гражданите да търсят отговорност от администраторите и да упражняват контрол над личните си данни[ii]. Тази цел се постига чрез въвеждане на специфични изисквания, които трябва да бъдат спазвани на всеки етап от обработването: преди началото на обработването или при събирането на личните данни и през целия период на обработването.

2.1. Елементи на прозрачността в GDPR (чл. 12)

2.1.1. "Кратка, прозрачна, разбираема и леснодостъпна форма"

Първите две части от това изискване означават, че администраторите трябва да предоставят информацията и да водят комуникацията с гражданите по ефикасен начин, в кратка форма, за да се избегне т.нар. „заливане с информация" (или казано по друг начин – да се претовари лицето с информация). Един вариант да се постигне това е чрез многопластови съобщения, чрез които субектите се информират за правата си постепенно (например може най-важната информация да се предостави в кратко съобщение, а останалата част – при самото събиране на данните (пр. при попълване на формуляр)). Тази информация трябва да бъде представена отделно от информацията, несвързана с защита на личните данни, като например договорни клаузи.

Изискването информацията да е „разбираема" означава, че тя следва да може да бъде разбирана от средностатистическия гражданин в съответната община. Гражданите трябва да могат предварително да определят какви са обхватът и последствията от обработването. Работната група по чл. 29 съветва администраторите да представят недвусмислено най-важните резултати от обработването, особено когато те може са засегнат основните човешки права на лицата[iii].

Последният елемент на прозрачността - „леснодостъпна форма" - следва да се разбира като липса на необходимост гражданите сами да търсят информация относно обработването на лични данни. Вместо това тя трябва да им е представена по лесен и достъпен начин, така че да могат да получат достъп до нея без полагането на каквито и да е било усилия.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

2.1.2. "Ясен и прост език"

Това изискване означава, че информацията трябва да бъде предоставена по най-простия възможен начин, като се избягват сложни езикови конструкции. Информацията не трябва да бъде формулирана с абстрактни или двузначни термини или пък да позволява различни тълкувания[iv]. Целите и правното основание за обработването трябва да са ясни. Неясни формулировки на целите на обработване, като „за развиване на бъдещи продукти и услуги" или „за проучване", трябва да се избягват. Информацията, предоставена на лицето, не трябва да съдържа твърде много правни, технически или специализирани термини[v].

По отношение на предоставяне на информация за обработване на лични данни на деца, местните власти трябва да се уверят, че лексиката, тонът и стилът на изразяване са подходящи и се възприемат от тях, така че те да могат да разберат, че съобщението/ информацията са насочени към тях[vi].

2.1.3. Начин на представяне на информацията (Чл. 12, пар. 1 и пар. 5 "безплатно")

Администраторите на лични данни не могат да таксуват гражданите за това, че им предоставят информация съгласно чл. 13 и чл. 14 (Информация, която се предоставя на субекта), или за съобщаване и действия, предприети с оглед чл. 15 – 22 (Права на субектите на данни) и чл. 34 (Съобщение за нарушения на сигурността на субектите на данни). Има само едно изключение от правилото: когато постъпилото искане от страна на дадено лице е явно неоснователно или прекомерно, по-специално поради повторяемост. В този случай администраторът може да наложи разумна такса, предвид административните разходи по предоставяне на информацията или по извършване на поисканото действие. Важно е общините, като администратори на лични данни, да съумеят да докажат явната неоснователност или прекомерността на искането. Следователно, не се препоръчва общините и другите органи на местната власт да налагат такси за предоставянето на информация по GDPR.

2.2. Информация, която трябва да се предостави на субектите (Чл. 13 и 14)

2.2.1. Каква информация трябва да се предостави?

Член 13 и член 14 от GDPR определят каква информация трябва да се предостави на лицата, чийто данни се обработват. Регламентът прави разлика между случаите, когато информацията е предоставена от лицето, и случаите, когато не е. Местните власти трябва да предоставят:

- данните, които идентифицират администратора и координатите за връзка с него;

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

- координатите за връзка с длъжностното лице по защита на данните;
- целите на обработването, за които личните данни са предназначени, както и правното основание за обработването – местните власти основно обработват лични данни на основния чл. 6, пар. 1, буква д) от GDPR, а именно при упражняване на официални правомощия, които са предоставени на администратора;
- получателите или категориите получатели на личните данни, ако има такива;
- данните, които идентифицират възможните получатели на данните – това не включва само трети лица, но и лицата, обработващи данните, както и съвместните администратори. Администраторът трябва да дефинира различните категории получатели на данни по най-конкретния възможен начин.

2.2.2. Каква допълнителна информация трябва да се предостави?

На първо място, за да е налице добросъвестно и прозрачно обработване, администраторът трябва да информира субекта за:

- периодът, за който данните ще се съхраняват или критериите, по които този период ще се определи;
- правото на всеки един гражданин да поиска от администратора достъп до информация или коригирането или изтриването ѝ, както и правото да се поиска ограничаване на обработването, да се направи възражение срещу обработването, както и правото на преносимост на данните;
- когато правното основание на обработването е съгласие, съществуването на правото на лицето да оттегли това съгласие по всяко време;
- правото на жалба до контролен орган;
- ако е приложимо - наличието на автоматизирано вземане на решения, включително профилиране, и важна информация за приложената логика, както и значението и възможните последствия за лицето от подобен тип обработване на данните.

Информацията за профилирането не само трябва да е леснодостъпна за субектите, но и да бъде представена на тяхното внимание. Администраторът трябва да уведоми субектите за логиката и критериите, използвани за автоматичното взимане на решения, като използва подходящ подход и достъпен език, без сложни обяснения на алгоритъма.

Когато данните не са получени пряко от определено лице, администраторът трябва да предостави информация кой е източника, предал личните данни. Ако

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

данните са получени пряко от определено лице, администраторът трябва да го уведоми дали обработването е в изпълнение на законово задължение.

Второ, администраторите трябва да информират гражданите, ако планират да обработват данни за други цели, извън тези, за които са събрани. Гражданите трябва да получат информация за тези други цели и всякаква по-нататъшна относима информация, подобна на информацията, която се предоставя за първоначалната цел (период на обработването, правно основание и др). Би било полезно да се информират лицата за евентуално бъдещо обработване още при първоначалното събиране на данните, ако е вероятно, че такова ще бъде осъществено предвид дейността на администратора.

2.2.3 Как трябва да се предостави информацията?

По подразбиране, формата за предоставяне на информация и комуникация с гражданите е писмена. GDPR обаче позволява информацията да бъде предоставена и по други начини, включително електронно. Според Работната група по чл. 29, важно е избраните методи да са съобразени с конкретната ситуация[vii]. Информацията може да бъде предоставена и устно при поискване от субекта, ако идентичността на субекта е доказана по други (не-устни) начини. От това правило има изключение по отношение на информацията, която администраторите трябва да предоставят по чл. 13 и чл. 14 – тя може да се предостави на субекта без проверка на идентичността. Устното предоставяне на информация не означава задължително устна информация, предоставена “на живо“. Този термин може да се разбира и като автоматизирана информация като предварително записана информация при телефонно обаждане. Според Работната група по чл. 29, администраторът трябва да осигури на субекта възможност да слуша повторно предварително записани съобщения, особено когато става дума за незрящи хора или хора с други трудности да възприемат информация в писмена форма. Също така, в случаи на устно представяне на информация, администраторите винаги трябва да могат да докажат, че се придържат към изискванията на GDPR. За да направят това, те трябва да пазят в архив: 1) искането на субекта да се предостави информация в устна форма, 2) методът, по който е проверена самоличността на лицето, и 3) фактът, че информацията е предоставена в устна форма[viii].

2.2.4 Кога се предоставя информация?

Информация относно обработването се дава на лицата в момента на събиране на данните (Чл. 13, пар. 1). Когато данните не се събират директно от гражданите, а от друг източник (например от държавна информационна система), информацията трябва да се предостави в разумен срок, но не по-късно от един месец от придобиването, в зависимост от обстоятелствата. Има два специфични

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

случая: първо, когато данните се използват за комуникация със лицето, информацията трябва да се предостави най-късно при първия контакт със него; второ, ако се очаква данните да се предоставят на друг получател, най-късно при първото им предоставяне на този друг получател.

2.2.5. Кога да се предостави съобщение в случай на промени в информацията по прозрачността, която администраторите трябва да предоставят?

В дадени ситуации, когато промяната в информацията може да има сериозен ефект върху определено лице, администраторът е длъжен да уведоми лицето в разумен срок преди промяната да бъде осъществена.[ix] Това уведомяване трябва да бъде изрично и ефективно. Гражданите трябва да имат на свое разположение достатъчно време да обмислят естеството и ефекта на промяната и да упражнят правата си по GDPR, като например да възразят срещу обработването. Работната група по чл. 29 препоръчва редовно уведомение на лицата относно обхвата на обработването[x].

Когато се планира да се обработват данни за други цели, извън тези, за които те са придобити, лицата трябва да се информират преди да е започнало новото обработване.

2.3. Условия

Условията на предоставяне на информация са начините, по които администраторите изпълняват задълженията си по GDPR да информират гражданите.

2.3.1. Съобщения относно нивото на защита на личните данни

По отношение на онлайн платформите, е препоръчително да се използват многопластови съобщения, които да пренасочват към различните категории информация, които трябва да се предоставят на лицата, вместо да се използва едно цялостно съобщение[xi]. Този подход позволява на потребителите да отидат директно на секцията от съобщението, която искат да прочетат. Когато се съставя подобно многопластово съобщение, администраторите трябва да се опитат да осигурят ясно и прегледно съдържание, така че субектите лесно да могат да разберат къде да намерят всяка част от информацията.

2.3.2. “Push” & “pull” уведомления

Работната група по чл. 29 препоръчва използване на “push” и “pull” уведомления. Основната разлика между двете е, че при вторите потребителите на сайта трябва сами да поискат информация, в случая такава за обработването на данните им, докато при първите съобщението изскача на екрана без активни действия от страна на потребителя. Работната група по чл. 29 дава примери за

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

"push" уведомления с т.нар. „навременни" уведомления, а за "pull" нотификации – с табла по прозрачността и указания тип „научи повече"[xii]:

- „навременно" уведомление се използва за предоставянето на специфична информация за защитата на личните данни, която се появява, когато е най-приложим за субекта. Този формат може да е полезен например когато местните власти имат сайт с определени онлайн услуги, които се използват чрез попълване на формуляр. Подобно „навременно" уведомление може да се появява преди гражданинът да попълни онлайн заявление;
- менюта относно прозрачността е мястото в онлайн среда, пр. сайт, където лицето може да види да промени настройките си относно поверителността на събраните лични данни, като позволи или забрани данните му да се използват по определени начини.

2.3.3. Други видове „подходящи мерки"

Според Работната група по чл. 29 извън виртуалната среда, подходящи мерки биха могли да са:

- при разпространение на хартиени копия – писмени обяснения, листовки;
- при телефонни разговори: устни обяснения от човек, автоматични предварително записани съобщения с опции да се чуе повече информация;
- QR кодове, гласови съобщения, писмени съобщения на smart устройство, съобщения по СМС, мейл и други;
- при личен контакт – устни обяснения, писмени обяснения в хартиен или електронен формат[xiii].

2.3.4. Визуализация

GDPR въвежда инструменти за визуализация (изреждайки по-конкретно икони, сертификати, печати и знаци за защита на личните данни). Идеята на иконите е да представят на субектите информацията по достъпен начин, използвайки стандартизирани символи/картинки, разпознаваеми в целия ЕС. Съставянето на такъв „кодекс с икони" все още не е започнало. GDPR въвежда също сертифициращи механизми при защитата на лични данни, печати и знаци, чрез които да се демонстрира съответствие с Регламента. Механизмите за сертификация се установяват от страните членки, от Европейския надзорен орган по защита на личните данни или от Комисията и целта им е администраторът да демонстрира спазването на изискванията на GDPR, предприемайки технически и организационни мерки, за да изпълни стандартите за защита на личните данни. Такива средства могат да се приложат при организации, които не са публични власти, като например общински дружества.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

2.4. Упражняване правата на гражданите

Гражданите имат право да получат информация от администраторите по отношение на обработването на личните им данни. Информацията, която трябва да се предостави по GDPR, е изрично изредена в чл. 13 и чл. 14, като лицата не следва да подават искане или да предприемат каквито и да било други стъпки, за да се сдобият с нея, за разлика от случаите, в които упражняват другите си права (право на достъп, право на коригиране, право на изтриване и други).

2.4.1. Изключения от задължението да се предостави информация

Правото на информация не е абсолютно, или казано по друг начин - то е ограничено в определени ситуации.

В някои случаи, местните власти нямат задължение да предоставят информацията, посочена в чл. 13 и 14 от Регламента. Когато данните са придобити пряко от гражданите, месните власти не е необходимо да предоставят информация, ако гражданите вече разполагат с такава (Чл. 13, пар. 4). Когато данните не са придобити директно от лицето, изключенията са повече (Чл. 14, пар. 5):

- когато лицето вече има такава информацията;
- когато предоставянето на такава информация се окаже невъзможно или изисква несъразмерно големи усилия, или ще направи изпълнението на целта на обработването невъзможно, или сериозно ще я затрудни - например ако администраторът на лични данните не разполага с никакви контакти на лицето;
- когато получаването или разкриването на лични данни е изрично разрешено от правото на ЕС или националното право, което ще е най-честата хипотеза за местните власти;
- когато личните данни са обект на задължение за пазене на служебна тайна според правото на ЕС или националното право, като такова включва всяко законово задължение за поверителност; това изключение може да се приложи в хипотеза на общински дружества и други подобни организации.

Според Работната група по чл. 29[xiv], като правило тези изключения могат да се тълкуват и прилагат само стеснително. Целта на тази препоръка е да се ограничат случаите, в които администраторите на данни могат да прилагат изключенията, и така да осигури по-голяма защита на правата на гражданите.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

3. ЗАКЛЮЧЕНИЕ И ПРАКТИЧЕСКИ СЪВЕТИ

Принципът на прозрачност е една от основите на GDPR. Той дава многобройни гаранции, че физическите лица ще могат да получат цялата информация, необходима за осведомяване относно обработваните личните данни, и за ефективното упражняване на правата по GDPR. Тази информация трябва да е лесна за разбиране и на ясен и прост език.

В тази връзка, съветът към местните власти е да изготвят списък с цялата информация, изисквана по GDPR, и да изберат най-добрите средства да достигнат до гражданите, чиито данни обработват. Например, могат да поставят плакати и табла с информация на общодостъпните места в сградите си и да разпространят листовки с информацията по чл. 13 и чл. 14. Електронните средства може да са полезни, ако организацията има онлайн сайт/платформа, но хартиените копия също са необходими в определени ситуации. Специално внимание трябва да се обърне на изискванията на GDPR в случаите, когато порталите на местните власти предоставят онлайн услуги. Трябва също да се има предвид, че някои общински дружества (като например дружества за обществен транспорт) извършват различни видове обработка на лични данни и работят с огромни бази данни, следователно трябва да положат особени усилия да съставят вярно информацията по чл. 13 и чл. 14.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

4. ВЪНШНИ ИЗТОЧНИЦИ И ЛИНКОВЕ

Книги

- Voigt, P., von dem Bussche, A., The EU General Data Protection Regulation (GDPR) – A Practical Guide, Springer International Publishing (2017);
- Bird & Bird Guide to General Data Protection Regulation (2016);
- EU General Data Protection Regulation (GDPR). An Implementation and Compliance Guide, IT Governance Publishing, Cambridgeshire (2016);

Документи на Работната група по чл. 29

- Работна група по чл. 24, Guidelines on Data Protection Officers ('DPOs'), WP 243 rev.01;
- Работна група по чл. 24, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, WP 217;

Онлайн връзки

- http://europa.eu/rapid/press-release_IP-18-386_en.htm
- https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en

5. ПРЕПРАТКИ

[i] Работната група по чл. 29 е основана на базата на чл. 29 от Директива 95/46/ЕС, която ще бъде заменена от GDPR. Целта на Работната група е да дава мнения, препоръки и съвети по отношение на защитата на личните данни.
[ii] Работна група по чл. 24, Guidelines on transparency under Regulation 2016/679, стр. 23
[iii] Пак там, стр. 8
[iv] Пак там, стр. 9
[v] Пак там
[vi] Пак там
[vii] Пак там, стр. 21
[viii] Пак там, стр. 12
[ix] Пак там, стр. 15
[x] Пак там, стр. 16
[xi] Пак там, стр. 17
[xii] Пак там, стр. 17-18
[xiii] Пак там, стр. 18-19
[xiv] Пак там, стр. 25

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

ProLegis

Разкриване на информация или право на достъп на субекта на данните - Член 15 GDPR

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

ProLegis

Съдържание

1. Правна рамка 3
   1.1. Общ регламент за защита на данните (GDPR) 3
2. Основни положения 5
3. Подробности за разкриването на информация на субекта на данните 6
   3.1. Същност на разкриването 6
   3.2. Колко време има администраторът да отговори (краен срок)? 7
   3.3. В каква форма може да бъде предявено искането и как да бъде отговорено? 7
   3.4. Трябва ли да бъде доказана самоличността на кандидата като обект на данните? 8
   3.5. Разходи? Може ли предоставянето на информацията да се заплаща? 9
   3.6. Има ли задължение заявителят да участва в разкриването на данни? 9
   3.7. Трябва ли правата на трети лица да се вземат предвид при предоставянето на информация? 9
4. Контролен списък за предоставяне на информация при поискване 10
   4.1. Предоставяне на информация 11
5. *Външни източници и интернет линкове* 13
   5.1. Книги и статии 13
   5.2. Други документи и дела 13

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

1. Правна рамка

1.1. Общ регламент за защита на данните (GDPR)

Член 15

Право на достъп на субекта на данните

1. Субектът на данните има право да получи от администратора потвърждение дали се обработват лични данни, свързани с него, и ако това е така, да получи достъп до данните и следната информация:

(а) целите на обработването;

(б) съответните категории лични данни;

(в) получателите или категориите получатели, пред които са или ще бъдат разкрити личните данни, по-специално получателите в трети държави или международни организации;

(г) когато е възможно, предвидения срок, за който ще се съхраняват личните данни, а ако това е невъзможно, критериите, използвани за определянето на този срок;

(д) съществуването на право да се изиска от администратора коригиране или изтриване на лични данни или ограничаване на обработването на лични данни, свързани със субекта на данните, или да се направи възражение срещу такова обработване;

(е) правото на жалба до надзорен;

(ж) когато личните данни не се събират от субекта на данните, всякаква налична информация за техния източник;

(з) съществуването на автоматизирано вземане на решения, включително профилирането, посочено в член 22, параграфи 1 и 4, и поне в тези случаи

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

съществена информация относно използваната логика, както и значението и предвидените последствия от това обработване за субекта на данните.

2. Когато личните данни се предават на трета държава или на международна организация, субектът на данните има право да бъде информиран относно подходящите гаранции по член 46 във връзка с предаването.

3. Администраторът предоставя копие от личните данни, които са в процес на обработване. За допълнителни копия, поискани от субекта на данните, администраторът може да наложи разумна такса въз основа на административните разходи. Когато субектът на данни подава искане с електронни средства, по възможност информацията се предоставя в широко използвана електронна форма, освен ако субектът на данни не е поискал друго.

4. Правото на получаване на копие, посочено в параграф 3, не влияе неблагоприятно върху правата и свободите на други лица.

Съображения 63 и 64:

(63) Всяко физическо лице следва да има право на достъп до събраните лични данни, които го засягат, и да упражнява това право лесно и на разумни интервали, за да бъде осведомено за обработването и да провери законосъобразността му. Това включва правото на субектите на данни на достъп до данните за здравословното им състояние, например данните в медицинските им досиета, които съдържат информация като диагнози, резултати от прегледи, становища на лекуващите лекари и проведени лечения или извършени операции. Поради това всеки субект на данни следва да има правото да е запознат и да получава информация, по-специално относно целите, за които се обработват личните данни, когато е възможно — срока, за който се обработват личните данни, получателите на личните данни, логиката на автоматизираното обработване на личните данни и последствията от такова обработване, най-малкото когато се извършва на основата на профилиране. Когато е възможно, администраторът следва да може да предоставя достъп от разстояние до сигурна система, която да предоставя на субекта на данните пряк достъп до неговите лични данни. Това право не следва да влияе неблагоприятно върху правата или свободите на други лица, включително върху търговската тайна или интелектуалната собственост, и по-специално върху авторското право за защита на софтуера. Тези съображения обаче не следва да представляват отказ за предоставяне на цялата информация на съответния субект на данни. Когато администраторът

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

обработва голямо количество информация относно субекта на данни, администраторът следва да може да поиска от субекта на данните, преди да бъде предадена информацията, да посочи точно информацията или дейностите по обработването, за които се отнася искането.

(64) Администраторът следва да използва всички разумни мерки за проверка на самоличността на субекта на данни, който иска достъп, по-специално по отношение на онлайн услугите и онлайн идентификаторите. Администраторът не следва да запазва лични данни с единствената цел да може да реагира на евентуални искания.

2. Основни положения

GDPR предвижда в член 15 правото на субекта на данни да получи достъп до цялата налична информация при надлежно направено искане (напр. клиент, служител, кандидат за работа, пациент, наричан по-долу "субект на данни“) до администратора (напр. компания, работодател, болница). Това се нарича "Право на достъп на субекта на данните (до неговите/нейните данни)“. Целта на това право е, субектът на данните да получи информация за съдържанието и подробностите относно обработваните за него данни, с цел евентуалното упражняване на други права (напр. корекция или заличаване съгласно член 16 GDPR) или да се направи една своеобразна проверка за законосъобразност на обработването.

Това право е един от фундаментите на правилата за защита на личните данни, защото често се приема като основа, върху която субектът на данните да стъпи при упражняването на други свои права. Надзорните органи, в рамките на GDPR, имат правомощието да извършват одити и проверки на работата на администраторите без да са сезирани с конкретна жалба. Въпреки това, на практика (поради ограничените ресурси на надзорните органи), обикновено е налице забавяне на предоставянето на информация на субектите на данни или техните искания изобщо не се адресират от страна на администратора, което изиграва ролята на покана към надзорния орган за извършване на проверка. Следователно, администраторите на данни трябва да бъдат добре подготвени за подобен сценарий.

Най-добрата подготовка за тези проверки е воденето на добре структурирани и възможно най-подробни регистри на дейностите по обработване. Колкото по-добре е оформена документацията относно процесите, при които се обработват лични данни, толкова по-лесно може да се намери и конкретната информация за конкретен обект при подаване на искания за достъп до информация

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

3. Подробности за разкриването на информация на субекта на данните

3.1. Същност на разкриването

Правото на достъп дава възможност на субекта на данни за следното:

i. право да поиска от администратора да потвърди дали данните му се обработват или не; следва лицето да получи отговор на запитването, дори и ако той е отрицателен, т.е. че не се обработват данни за този човек (така наречената "отрицателна информация"): "Ние не обработваме данни за вас";

ii. правото да се получи копие от личните данни, които са предмет на обработване (за допълнителни копия, поискани от субекта на данните, администраторът може да наложи разумна такса въз основа на административните разходи.) Ако лицето, подало данните, подаде заявлението по електронен път, информацията се предоставя също в електронен формат, освен ако не е посочено друго.

iii. правото да получи следната информация:

Член 15, параграф 1 GDPR	**Съдържание на информацията**
а)	**целите на обработването**;
б)	съответните **категории** лични данни, които се обработват;
в)	**получателите или категориите получатели**, пред които са или ще бъдат разкрити личните данни, по-специално получателите в трети държави или международни организации;
г)	когато е възможно, **предвидения срок, за който ще се съхраняват личните данни**, а ако това е невъзможно - критериите, използвани за определянето на този срок;
д)	**съществуването на право да се изиска от администратора коригиране или изтриване на лични данни или ограничаване на обработването на лични данни**, свързани със субекта на данните, или да се направи възражение срещу такова обработване;
е)	**правото на жалба** до надзорен орган;
ж)	когато личните данни не се събират от субекта на данните, **всякаква налична информация за техния източник**;
з)	съществуването на **автоматизирано вземане на решения**, включително профилирането, посочено в

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

	член 22, параграфи 1 и 4, и поне в тези случаи съществена информация относно използваната логика, както и значението и предвидените последствия от това обработване за субекта на данните.
Ал.2	Когато личните данни **се предават на трета държава или на международна организация**, субектът на данните има право да бъде информиран относно подходящите гаранции по член 46 във връзка с предаването.

Забележка: Съгласно член 23 **правото на информация може да бъде ограничено от националното законодателство.**

3.2. Колко време има администраторът да отговори (краен срок)?

По принцип, на подадено заявление за достъп до информация трябва да бъде отговорено своевременно, но не по-късно от един месец след получаване на заявлението (член 12, пар. 3 от GDPR). Този период може да бъде удължен за още два месеца, ако е необходимо, като се вземат предвид сложността и броят на заявленията. Администраторът уведомява субекта на данни за удължаването на крайния срок в рамките на един месец след получаване на искането, заедно с причините за забавянето. Ако заинтересованото лице подаде заявлението по електронен път, субектът на данните се информира по електронен път, освен ако не е посочено друго.

Ако администраторът няма да отговори на искането на субекта на данните, той незабавно следва да информира субекта на данните, но не по-късно от един месец след получаване на искането, относно причините за това и възможността да подаде жалба до надзорен орган или да предяви иск пред компетентен съд.

3.3. В каква форма може да бъде предявено искането и как да бъде отговорено?

Регламентът не съдържа изискване за формата, в която следва да бъде направено заявлението. Искането може да бъде направено устно, писмено или в електронен формат (например чрез електронна поща). Администраторът може да предостави исканата информация във всяка подходяща форма, но следва да се отбележи следното:

- най-добре е на писмено заявление също да бъде отговорено писмено. Общ похват, използван в миналото, е, че заявителят трябва да подаде копие от документ за самоличност към своето заявление, а администраторът да изпрати отговора като препоръчано писмо. Въпреки това, тъй като документа за самоличност обикновено съдържа по-голям

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

обем от лични данни от необходимото за идентифицирането на субекта на данни, се препоръчва в писмена форма да се предоставя само информация относно име, единен граждански номер и/ или серийния номер на документа за самоличност от субекта на данните;

- ако заявителя поиска, информацията може да бъде предоставена устно, при условие че идентичността на субекта на данните е установена в друга форма (напр. субектът на данни се е идентифицирал с документ за самоличност); .
- ако субектът на данните подаде заявление по електронен път (например чрез електронна поща), информацията също се предоставя в електронен формат, освен ако не е посочено друго. Ако е възможно, администраторът може също да предостави отдалечен достъп до сигурна система, която дава на субекта на данни пряк достъп до личната му информация.

Внимание! Цялата комуникация между администратора и субекта на данни трябва да се води на **ясен и прост език** в точна, прозрачна, разбираема и леснодостъпна форма (това важи особено за информация, насочена специално към децата). Например, ако администратора предоставя информация, която включва употребата на съкращения и абревиатури, те следва да бъдат подробно обяснени от администратора в неговия отговор.

3.4. Трябва ли да бъде доказана самоличността на кандидата като обект на данните?

Идентичността на лицето, което иска информацията (заинтересованото лице), трябва да е установена, като администраторът може да поиска допълнителна информация, ако има "основателни съмнения" относно самоличността на физическото лице, подало заявлението (вж. чл.12, ал.6[1]).

Съгласно съображение 64 администраторът следва да използва всички разумни мерки за проверка на самоличността на субекта на данни, който иска достъп, по-специално по отношение в областта на онлайн услугите и онлайн идентификаторите.

Ако се използва система юза идентификация на самоличността на физическите лица, тя трябва да бъде разработена по начин, който гарантира сигурността на данните в съответствие с риска. В противен случай може да възникне нарушение на сигурността на личните данни, ако те бъдат предадени на грешния получател.

Например, обичайна практика в Австрия, съгласно предходния Закон за защита на личните данни (DSG 2000), е, подаването от заявителя на копие от

[1] Вж. също Souhrada-Kirchmayer, The right of access to the GDPR, in Jahnel [Hrsg], Yearbook 17. Data Protection Law [2017].

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

документ за самоличност към заявлението за достъп до информация, а администраторът, от своя страна, връща отговор по пощата като препоръчано писмо. В зависимост от конкретната ситуация, самоличността на дадено физическо лице може да е ясна, напр. ако има постоянни отношения с администратора и последният няма необходимост да го идентифицира специално за тази цел[2].

3.5. Разходи? Може ли предоставянето на информацията да се заплаща?

По принцип, информацията трябва да бъде предоставена безплатно (вж. член 12, пар. 5 от GDPR). Въпреки това, в случай на явно неоснователни или по-специално повтарящи се прекомерни искания от страна на субекта на данни, администраторът може да:

- наложи разумна такса, като се вземат предвид административните разходи за уведомяване, съобщаване или прилагане на исканата мярка; или
- откаже да действа по заявлението.

3.6. Има ли задължение заявителят да участва в разкриването на данни?

Да, дори ако задължението за сътрудничество е споменато само в съображение 63, в доктрината се приема, че такова съществува (така също беше признато в Австрия съгласно DSG 2000): "където администраторът обработва голямо количество от информация, отнасяща се до субекта на данни, той трябва да може да поиска от субекта на данни да определи информацията или дейностите по обработването, за които се отнася искането, преди предоставянето на пълната информация."[3]

3.7. Трябва ли правата на трети лица да се вземат предвид при предоставянето на информация?

Да, съгласно член 15, пар. 4 от GDPR, правото да се получи копие, не трябва влияе неблагоприятно върху правата и свободите на други лица. Освен това, съображение 63 гласи, че *"[т]ова право не следва да влияе неблагоприятно върху правата или свободите на други лица, включително върху търговската тайна или интелектуалната собственост, и по-специално върху авторското право за*

[2] Вж. пр. практиката на Висшите австрийски съдилища: VwGH 4.7.2016, Ra 2016/04/0014; OGH 25.2.1993, 6 Ob 6/93)

[3] Съображение 63

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

защита на софтуера. Тези съображения обаче не следва да представляват отказ за предоставяне на цялата информация на съответния субект на данни."

Поради това е необходимо да се упражнява контрол върху данните, които се разкриват. Като правило личните данни на трети лица (пр., името на лицето, което обслужва клиента, посочено в клиентски файл), трябва да бъдат изтрити от копието на лични данни, което ще се предостави на заявителя.

4. Контролен списък за предоставяне на информация при поискване

Задължен ли съм да предоставям информация?	Ако публичен орган (пр. община) е администратор на лични данни - ДА. Ако публичен орган е само обработващ, но все пак получава молба, тя трябва незабавно да я препрати на отговорното лице.
Проверка на самоличност	Самоличността на лицето, поискало информацията (заинтересованото лице), трябва да е ясна. Ако има съмнения относно самоличността: поискване на доказателство – предоставяне на документ за самоличност.
Разкриването на информация безплатно ли е?	По принцип - ДА. Ако на заявителя често е давана една и същата информация или ако искането сериозно затруднява администратора, е възможно да се наложи административна такса. NB! Този въпрос е предмет на националното законодателство. Следва да се следи приложимото законодателство към конкретната дейност по обработване.
Обработват ли се въобще лични данни на заявителя?	Ако не са съхраняват данни или ако данните вече са били изтрити, или данните са били безвъзвратно унищожени, то тогава няма да бъдат обработвани лични данни и ще бъде

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

	предоставена т. нар. негативна информация - "Ние не обработваме данни за Вас".
Какви данни и информация трябва да предостави администраторът?	Трябва да се предоставят всички данни, които се съхраняват за съответното лице. В зависимост от сложността на системите, трябва да се вземе предвид предварително (с оглед на конкретната област на обработването), в кои системи се съхраняват какви категории данни относно засегнатите лица. Освен това трябва да се предостави информацията, посочена в член 15, пар. 1 от GDPR. Трябва да се спазват правата на трети лица (особено търговските тайни и данните на трети страни трябва да бъдат изтрити / заличени).

4.1. Предоставяне на информация

Пример за достъп до информация съгласно член 15 от GDPR

Уважаеми господине / госпожо [име],

1. В отговор на Вашето заявление от [дата] за информация съгласно чл. 15 GDPR, получена от нас на [дата], може да се отговори, както следва:

2. [В случай на отговор в рамките на един месец от получаването] Потвърждаваме своевременно, че обработваме лични данни за Вас.

[в случай на удължаване съгласно чл. 12 (3) GDPR] Както е посочено в писмото от [дата], се възползвахме от възможността да удължим крайния срок до три месеца поради [сложността на молбата или броя на Вашите искания, необходимо е допълнително обяснение].

3. [ако не се обработват данни] Не се обработват лични данни за Вас. [След това продължете с текстовия модул № 9].

[Когато се обработват данни] Обработваме следните категории данни за Вас: [списък на категориите данни, които се обработват].

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

Справка за / копие от документите относно съответното действие по обработване на лични данни е в приложение към настоящия документ. Всяко заличаване се отнася до лични данни на трети лица така, че да не се засягат правата и интересите им.

4. [Ако данните не са събрани пряко от субекта на данните]: Получихме данните Ви от [наличната информация за произхода на вашите данни, напр. публичен орган XY].

5. [ако е приложимо] Ще използваме автоматизирани процедури за вземане на решения / процедури по профилиране, които имат правни последствия спрямо Вас или Ви засягат по подобен начин: [моля, попълнете информация за използваната логика и съответните последствия].

6. Имате право на коригиране, заличаване, ограничаване и право на възражение срещу обработването на личните Ви данни. В такъв случай свържете се с нас. Ако смятате, че обработването на данните Ви, нарушава Закона за защита на данните или ако исканията Ви за защита на данните са били нарушени по някакъв начин, можете да подадете жалба до надзорния орган. Отговорният орган в България е Комисия за защита на личните данни.

С уважение

....

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

5. *Външни източници и интернет линкове*

5.1. Книги и статии

- Souhrada-Kirchmayer, The right of access to the DSGVO, in Jahnel [Hrsg], Yearbook 17. Data Protection Law [2017] 86 f.
- *Martini in Paal/Pauly* (Ed.), Datenschutz-Grundverordnung (2016).

5.2. Други документи и дела

- jurisprudence of the Austrian High Courts: VwGH 4.7.2016, Ra 2016/04/0014; OGH 25.2.1993, 6 Ob 6/93) Web Links
- За сравнение с правния режим по Директива 95/46/ЕО, вж. https://gdpr.report/news/2017/11/20/gdpr-subject-access-requests/

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

ProLegis

RECHTLICHE GRÜNDE FÜR DIE VERARBEITUNG PERSONENBEZOGENER DATEN

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

Dissemination Level:		
PU	Public	
CO	Confidential, only for members of the consortium (including the Commission Services)	
EU-RES	Classified Information: RESTREINT UE (Commission Decision 2005/444/EC)	
EU-CON	Classified Information: CONFIDENTIEL UE (Commission Decision 2005/444/EC)	
EU-SEC	Classified Information: SECRET UE (Commission Decision 2005/444/EC)	
Document version control:		
Version	**Author(s)**	**Date**
Version 1	Developed by:	
Version 1	Reviewed & updated by:	
Version 2	Translated by: VICESSE	21/06/18

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

Inhaltsverzeichnis

1. RECHTLICHER RAHMEN 5
1.1. Charta der Grundrechte der EU 5
1.2. DSGVO 5
2. RECHTLICHMÄSSIGE GRÜNDE FÜR DIE VERARBEITUNG PERSONENBEZOGENER DATEN IM RAHMEN DER DSGVO 12
2.1. Zustimmung 12
2.1.1. Bedeutung und rechtliche Grundlagen 12
2.1.2. Anwendbarkeit im Rahmen der Tätigkeit der lokalen Behörden 14
2.2. Erfüllung / Vertragsschluss mit der betroffenen Person 16
2.2.1. Bedeutung und rechtliche Anforderungen 16
2.2.2. Anwendbarkeit im Rahmen der Tätigkeit der lokalen Behörden 17
2.3. Rechtliche Verpflichtung 18
2.3.1. Bedeutung und rechtliche Anforderungen 18
2.3.2. Anwendbarkeit im Rahmen der Tätigkeit der örtlichen Behörden 19
2.4. Lebenswichtige Interessen 19
2.4.2. Anwendbarkeit im Rahmen der Tätigkeit der örtlichen Behörden 20
2.5. Aufgabe im öffentlichen Interesse 21
2.5.1. Bedeutung und rechtliche Anforderungen 21
2.5.2. Anwendbarkeit im Rahmen der Tätigkeit der örtlichen Behörden 22
2.6. Legitime Interessen 22
2.6.1. Bedeutung und rechtliche Anforderungen 22
2.6.2. Anwendbarkeit im Rahmen der Tätigkeit der örtlichen Behörden 24
3. SCHLUSSFOLGERUNG & PRAKTISCHE HINWEISE 24
4. EXTERNE QUELLEN & WEBLINKS 25
4.1. Bücher 25
4.2. Dokumente der Artikel 29 Working Party 25
4.3. Web Links 25

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

5. REFERENZEN 26

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

1. RECHTLICHER RAHMEN

1.1. Charta der Grundrechte der EU

Artikel 8

Schutz personenbezogener Daten

(1) Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten.

(2) Diese Daten dürfen nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der

betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet wer- den. Jede Person hat das Recht, Auskunft über die sie betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu erwirken.

(3) Die Einhaltung dieser Vorschriften wird von einer unabhängigen Stelle überwacht.

1.2. DSGVO

Artikel 4

Begriffsbestimmungen

Im Sinne dieser Verordnung bezeichnet der Ausdruck:

[…]

11. „Einwilligung“ der betroffenen Person jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist;

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

Artikel 6

Rechtmäßigkeit der Verarbeitung

(1) Die Verarbeitung ist nur rechtmäßig, wenn mindestens eine der nachstehenden Bedingungen erfüllt ist:

a) Die betroffene Person hat ihre Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben;

b) die Verarbeitung ist für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich, die auf Anfrage der betroffenen Person erfolgen;

c) die Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich, der der Verantwortliche unterliegt;

d) die Verarbeitung ist erforderlich, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen;

e) die Verarbeitung ist für die Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde;

f) die Verarbeitung ist zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt.

Unterabsatz 1 Buchstabe f gilt nicht für die von Behörden in Erfüllung ihrer Aufgaben vorgenommene Verarbeitung.

(2) Die Mitgliedstaaten können spezifischere Bestimmungen zur Anpassung der Anwendung der Vorschriften dieser Verordnung in Bezug auf die Verarbeitung zur Erfüllung von Absatz 1 Buchstaben c und e beibehalten oder einführen, indem sie spezifische Anforderungen für die Verarbeitung sowie sonstige Maßnahmen präziser bestimmen, um eine rechtmäßig und nach Treu und Glauben erfolgende Verarbeitung zu gewährleisten, einschließlich für andere besondere Verarbeitungssituationen gemäß Kapitel IX.

(3) Die Rechtsgrundlage für die Verarbeitungen gemäß Absatz 1 Buchstaben c und e wird festgelegt durch

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

a) Unionsrecht oder

b) das Recht der Mitgliedstaaten, dem der Verantwortliche unterliegt.

Der Zweck der Verarbeitung muss in dieser Rechtsgrundlage festgelegt oder hinsichtlich der Verarbeitung gemäß Absatz 1 Buchstabe e für die Erfüllung einer Aufgabe erforderlich sein, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde. Diese Rechtsgrundlage kann spezifische Bestimmungen zur Anpassung der Anwendung der Vorschriften dieser Verordnung enthalten, unter anderem Bestimmungen darüber, welche allgemeinen Bedingungen für die Regelung der Rechtmäßigkeit der Verarbeitung durch den Verantwortlichen gelten, welche Arten von Daten verarbeitet werden, welche Personen betroffen sind, an welche Einrichtungen und für welche Zwecke die personenbezogenen Daten offengelegt werden dürfen, welcher Zweckbindung sie unterliegen, wie lange sie gespeichert werden dürfen und welche Verarbeitungsvorgänge und -verfahren angewandt werden dürfen, einschließlich Maßnahmen zur Gewährleistung einer rechtmäßig und nach Treu und Glauben erfolgenden Verarbeitung, wie solche für sonstige besondere Verarbeitungssituationen gemäß Kapitel IX. Das Unionsrecht oder das Recht der Mitgliedstaaten müssen ein im öffentlichen Interesse liegendes Ziel verfolgen und in einem angemessenen Verhältnis zu dem verfolgten legitimen Zweck stehen.

(4) Beruht die Verarbeitung zu einem anderen Zweck als zu demjenigen, zu dem die personenbezogenen Daten erhoben wurden, nicht auf der Einwilligung der betroffenen Person oder auf einer Rechtsvorschrift der Union oder der Mitgliedstaaten, die in einer demokratischen Gesellschaft eine notwendige und verhältnismäßige Maßnahme zum Schutz der in Artikel 23 Absatz 1 genannten Ziele darstellt, so berücksichtigt der Verantwortliche — um festzustellen, ob die Verarbeitung zu einem anderen Zweck mit demjenigen, zu dem die personenbezogenen Daten ursprünglich erhoben wurden, vereinbar ist — unter anderem

a) jede Verbindung zwischen den Zwecken, für die die personenbezogenen Daten erhoben wurden, und den Zwecken der beabsichtigten Weiterverarbeitung,

b) den Zusammenhang, in dem die personenbezogenen Daten erhoben wurden, insbesondere hinsichtlich des Verhältnisses zwischen den betroffenen Personen und dem Verantwortlichen,

c) die Art der personenbezogenen Daten, insbesondere ob besondere Kategorien personenbezogener Daten gemäß Artikel 9 verarbeitet werden oder ob

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

personenbezogene Daten über strafrechtliche Verurteilungen und Straftaten gemäß Artikel 10 verarbeitet werden,

d) die möglichen Folgen der beabsichtigten Weiterverarbeitung für die betroffenen Personen,

e) das Vorhandensein geeigneter Garantien, wozu Verschlüsselung oder Pseudonymisierung gehören kann.

Erwägungsgründe

(42) Erfolgt die Verarbeitung mit Einwilligung der betroffenen Person, sollte der Verantwortliche nachweisen können, dass die betroffene Person ihre Einwilligung zu dem Verarbeitungsvorgang gegeben hat. Insbesondere bei Abgabe einer schriftlichen Erklärung in anderer Sache sollten Garantien sicherstellen, dass die betroffene Person weiß, dass und in welchem Umfang sie ihre Einwilligung erteilt. Gemäß der Richtlinie 93/13/EWG des Rates (10) sollte eine vom Verantwortlichen vorformulierte Einwilligungserklärung in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zur Verfügung gestellt werden, und sie sollte keine missbräuchlichen Klauseln beinhalten. Damit sie in Kenntnis der Sachlage ihre Einwilligung geben kann, sollte die betroffene Person mindestens wissen, wer der Verantwortliche ist und für welche Zwecke ihre personenbezogenen Daten verarbeitet werden sollen. Es sollte nur dann davon ausgegangen werden, dass sie ihre Einwilligung freiwillig gegeben hat, wenn sie eine echte oder freie Wahl hat und somit in der Lage ist, die Einwilligung zu verweigern oder zurückzuziehen, ohne Nachteile zu erleiden.

(43) Um sicherzustellen, dass die Einwilligung freiwillig erfolgt ist, sollte diese in besonderen Fällen, wenn zwischen der betroffenen Person und dem Verantwortlichen ein klares Ungleichgewicht besteht, insbesondere wenn es sich bei dem Verantwortlichen um eine Behörde handelt, und es deshalb in Anbetracht aller Umstände in dem speziellen Fall unwahrscheinlich ist, dass die Einwilligung freiwillig gegeben wurde, keine gültige Rechtsgrundlage liefern. Die Einwilligung gilt nicht als freiwillig erteilt, wenn zu verschiedenen Verarbeitungsvorgängen von personenbezogenen Daten nicht gesondert eine Einwilligung erteilt werden kann, obwohl dies im Einzelfall angebracht ist, oder wenn die Erfüllung eines Vertrags, einschließlich der Erbringung einer Dienstleistung, von der Einwilligung abhängig ist, obwohl diese Einwilligung für die Erfüllung nicht erforderlich ist.

(44) Die Verarbeitung von Daten sollte als rechtmäßig gelten, wenn sie für die Erfüllung oder den geplanten Abschluss eines Vertrags erforderlich ist.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

(45) Erfolgt die Verarbeitung durch den Verantwortlichen aufgrund einer ihm obliegenden rechtlichen Verpflichtung oder ist die Verarbeitung zur Wahrnehmung einer Aufgabe im öffentlichen Interesse oder in Ausübung öffentlicher Gewalt erforderlich, muss hierfür eine Grundlage im Unionsrecht oder im Recht eines Mitgliedstaats bestehen. Mit dieser Verordnung wird nicht für jede einzelne Verarbeitung ein spezifisches Gesetz verlangt. Ein Gesetz als Grundlage für mehrere Verarbeitungsvorgänge kann ausreichend sein, wenn die Verarbeitung aufgrund einer dem Verantwortlichen obliegenden rechtlichen Verpflichtung erfolgt oder wenn die Verarbeitung zur Wahrnehmung einer Aufgabe im öffentlichen Interesse oder in Ausübung öffentlicher Gewalt erforderlich ist. Desgleichen sollte im Unionsrecht oder im Recht der Mitgliedstaaten geregelt werden, für welche Zwecke die Daten verarbeitet werden dürfen. Ferner könnten in diesem Recht die allgemeinen Bedingungen dieser Verordnung zur Regelung der Rechtmäßigkeit der Verarbeitung personenbezogener Daten präzisiert und es könnte darin festgelegt werden, wie der Verantwortliche zu bestimmen ist, welche Art von personenbezogenen Daten verarbeitet werden, welche Personen betroffen sind, welchen Einrichtungen die personenbezogenen Daten offengelegt, für welche Zwecke und wie lange sie gespeichert werden dürfen und welche anderen Maßnahmen ergriffen werden, um zu gewährleisten, dass die Verarbeitung rechtmäßig und nach Treu und Glauben erfolgt. Desgleichen sollte im Unionsrecht oder im Recht der Mitgliedstaaten geregelt werden, ob es sich bei dem Verantwortlichen, der eine Aufgabe wahrnimmt, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, um eine Behörde oder um eine andere unter das öffentliche Recht fallende natürliche oder juristische Person oder, sofern dies durch das öffentliche Interesse einschließlich gesundheitlicher Zwecke, wie die öffentliche Gesundheit oder die soziale Sicherheit oder die Verwaltung von Leistungen der Gesundheitsfürsorge, gerechtfertigt ist, eine natürliche oder juristische Person des Privatrechts, wie beispielsweise eine Berufsvereinigung, handeln sollte.

(46) Die Verarbeitung personenbezogener Daten sollte ebenfalls als rechtmäßig angesehen werden, wenn sie erforderlich ist, um ein lebenswichtiges Interesse der betroffenen Person oder einer anderen natürlichen Person zu schützen. Personenbezogene Daten sollten grundsätzlich nur dann aufgrund eines lebenswichtigen Interesses einer anderen natürlichen Person verarbeitet werden, wenn die Verarbeitung offensichtlich nicht auf eine andere Rechtsgrundlage gestützt werden kann. Einige Arten der Verarbeitung können sowohl wichtigen Gründen des öffentlichen Interesses als auch lebenswichtigen Interessen der betroffenen Person dienen; so kann beispielsweise die Verarbeitung für humanitäre Zwecke einschließlich der Überwachung von Epidemien und deren Ausbreitung oder in humanitären Notfällen insbesondere bei Naturkatastrophen oder vom Menschen verursachten Katastrophen erforderlich sein.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

(47) Die Rechtmäßigkeit der Verarbeitung kann durch die berechtigten Interessen eines Verantwortlichen, auch eines Verantwortlichen, dem die personenbezogenen Daten offengelegt werden dürfen, oder eines Dritten begründet sein, sofern die Interessen oder die Grundrechte und Grundfreiheiten der betroffenen Person nicht überwiegen; dabei sind die vernünftigen Erwartungen der betroffenen Person, die auf ihrer Beziehung zu dem Verantwortlichen beruhen, zu berücksichtigen. Ein berechtigtes Interesse könnte beispielsweise vorliegen, wenn eine maßgebliche und angemessene Beziehung zwischen der betroffenen Person und dem Verantwortlichen besteht, z. B. wenn die betroffene Person ein Kunde des Verantwortlichen ist oder in seinen Diensten steht. Auf jeden Fall wäre das Bestehen eines berechtigten Interesses besonders sorgfältig abzuwägen, wobei auch zu prüfen ist, ob eine betroffene Person zum Zeitpunkt der Erhebung der personenbezogenen Daten und angesichts der Umstände, unter denen sie erfolgt, vernünftigerweise absehen kann, dass möglicherweise eine Verarbeitung für diesen Zweck erfolgen wird. Insbesondere dann, wenn personenbezogene Daten in Situationen verarbeitet werden, in denen eine betroffene Person vernünftigerweise nicht mit einer weiteren Verarbeitung rechnen muss, könnten die Interessen und Grundrechte der betroffenen Person das Interesse des Verantwortlichen überwiegen. Da es dem Gesetzgeber obliegt, per Rechtsvorschrift die Rechtsgrundlage für die Verarbeitung personenbezogener Daten durch die Behörden zu schaffen, sollte diese Rechtsgrundlage nicht für Verarbeitungen durch Behörden gelten, die diese in Erfüllung ihrer Aufgaben vornehmen. Die Verarbeitung personenbezogener Daten im für die Verhinderung von Betrug unbedingt erforderlichen Umfang stellt ebenfalls ein berechtigtes Interesse des jeweiligen Verantwortlichen dar. Die Verarbeitung personenbezogener Daten zum Zwecke der Direktwerbung kann als eine einem berechtigten Interesse dienende Verarbeitung betrachtet werden.

(48) Verantwortliche, die Teil einer Unternehmensgruppe oder einer Gruppe von Einrichtungen sind, die einer zentralen Stelle zugeordnet sind können ein berechtigtes Interesse haben, personenbezogene Daten innerhalb der Unternehmensgruppe für interne Verwaltungszwecke, einschließlich der Verarbeitung personenbezogener Daten von Kunden und Beschäftigten, zu übermitteln. Die Grundprinzipien für die Übermittlung personenbezogener Daten innerhalb von Unternehmensgruppen an ein Unternehmen in einem Drittland bleiben unberührt.

(49) Die Verarbeitung von personenbezogenen Daten durch Behörden, Computer-Notdienste (Computer Emergency Response Teams — CERT, beziehungsweise Computer Security Incident Response Teams — CSIRT), Betreiber von elektronischen Kommunikationsnetzen und -diensten sowie durch Anbieter von Sicherheitstechnologien und -diensten stellt in dem Maße ein berechtigtes Interesse des jeweiligen Verantwortlichen

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

dar, wie dies für die Gewährleistung der Netz- und Informationssicherheit unbedingt notwendig und verhältnismäßig ist, d.h. soweit dadurch die Fähigkeit eines Netzes oder Informationssystems gewährleistet wird, mit einem vorgegebenen Grad der Zuverlässigkeit Störungen oder widerrechtliche oder mutwillige Eingriffe abzuwehren, die die Verfügbarkeit, Authentizität, Vollständigkeit und Vertraulichkeit von gespeicherten oder übermittelten personenbezogenen Daten sowie die Sicherheit damit zusammenhängender Dienste, die über diese Netze oder Informationssysteme angeboten werden bzw. zugänglich sind, beeinträchtigen. Ein solches berechtigtes Interesse könnte beispielsweise darin bestehen, den Zugang Unbefugter zu elektronischen Kommunikationsnetzen und die Verbreitung schädlicher Programmcodes zu verhindern sowie Angriffe in Form der gezielten Überlastung von Servern („Denial of service"-Angriffe) und Schädigungen von Computer- und elektronischen Kommunikationssystemen abzuwehren.

(50) Die Verarbeitung personenbezogener Daten für andere Zwecke als die, für die die personenbezogenen Daten ursprünglich erhoben wurden, sollte nur zulässig sein, wenn die Verarbeitung mit den Zwecken, für die die personenbezogenen Daten ursprünglich erhoben wurden, vereinbar ist. In diesem Fall ist keine andere gesonderte Rechtsgrundlage erforderlich als diejenige für die Erhebung der personenbezogenen Daten. Ist die Verarbeitung für die Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde, so können im Unionsrecht oder im Recht der Mitgliedstaaten die Aufgaben und Zwecke bestimmt und konkretisiert werden, für die eine Weiterverarbeitung als vereinbar und rechtmäßig erachtet wird. Die Weiterverarbeitung für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke sollte als vereinbarer und rechtmäßiger Verarbeitungsvorgang gelten. Die im Unionsrecht oder im Recht der Mitgliedstaaten vorgesehene Rechtsgrundlage für die Verarbeitung personenbezogener Daten kann auch als Rechtsgrundlage für eine Weiterverarbeitung dienen. Um festzustellen, ob ein Zweck der Weiterverarbeitung mit dem Zweck, für den die personenbezogenen Daten ursprünglich erhoben wurden, vereinbar ist, sollte der Verantwortliche nach Einhaltung aller Anforderungen für die Rechtmäßigkeit der ursprünglichen Verarbeitung unter anderem prüfen, ob ein Zusammenhang zwischen den Zwecken, für die die personenbezogenen Daten erhoben wurden, und den Zwecken der beabsichtigten Weiterverarbeitung besteht, in welchem Kontext die Daten erhoben wurden, insbesondere die vernünftigen Erwartungen der betroffenen Person, die auf ihrer Beziehung zu dem Verantwortlichen beruhen, in Bezug auf die weitere Verwendung dieser Daten, um welche Art von personenbezogenen Daten es sich handelt, welche Folgen die beabsichtigte Weiterverarbeitung für die betroffenen

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

Personen hat und ob sowohl beim ursprünglichen als auch beim beabsichtigten Weiterverarbeitungsvorgang geeignete Garantien bestehen.

Hat die betroffene Person ihre Einwilligung erteilt oder beruht die Verarbeitung auf Unionsrecht oder dem Recht der Mitgliedstaaten, was in einer demokratischen Gesellschaft eine notwendige und verhältnismäßige Maßnahme zum Schutz insbesondere wichtiger Ziele des allgemeinen öffentlichen Interesses darstellt, so sollte der Verantwortliche die personenbezogenen Daten ungeachtet der Vereinbarkeit der Zwecke weiterverarbeiten dürfen. In jedem Fall sollte gewährleistet sein, dass die in dieser Verordnung niedergelegten Grundsätze angewandt werden und insbesondere die betroffene Person über diese anderen Zwecke und über ihre Rechte einschließlich des Widerspruchsrechts unterrichtet wird. Der Hinweis des Verantwortlichen auf mögliche Straftaten oder Bedrohungen der öffentlichen Sicherheit und die Übermittlung der maßgeblichen personenbezogenen Daten in Einzelfällen oder in mehreren Fällen, die im Zusammenhang mit derselben Straftat oder derselben Bedrohung der öffentlichen Sicherheit stehen, an eine zuständige Behörde sollten als berechtigtes Interesse des Verantwortlichen gelten. Eine derartige Übermittlung personenbezogener Daten im berechtigten Interesse des Verantwortlichen oder deren Weiterverarbeitung sollte jedoch unzulässig sein, wenn die Verarbeitung mit einer rechtlichen, beruflichen oder sonstigen verbindlichen Pflicht zur Geheimhaltung unvereinbar ist.

2. RECHTLICHMÄSSIGE GRÜNDE FÜR DIE VERARBEITUNG PERSONENBEZOGENER DATEN IM RAHMEN DER DSGVO

2.1. Zustimmung

2.1.1. Bedeutung und rechtliche Grundlagen

Die Einwilligung ist einer der sechs rechtsmäßigen Gründe gemäß Art. 6 der DSGVO. Um gültig zu sein, erfordert die DSGVO, dass die Zustimmung frei gegeben, spezifisch, informiert und eindeutig ist.

- "frei" bedeutet eine echte Wahl und Kontrolle für die betroffenen Personen.[i] Treten für die betroffene Person nachteilige Folgen auf, falls sie der

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

Verarbeitung nicht zustimmen / zurücktreten, so wird die Einwilligung nicht berücksichtigt (z. B. Dienstverweigerung, höhere Kosten für Waren / Dienstleistungen - Gebühren, Preis usw.) bzw. ist die Zustimmung nicht frei gegeben. Aufgrund der Unausgewogenheit der Zuständigkeiten zwischen Behörden und betroffenen Personen wäre die Einwilligung nur selten ein nützliches Instrument für die Datenverarbeitung im Rahmen der Ausübung öffentlicher Behörden;

- "spezifisch" = eng mit der Anforderung verbunden ist, dass die betroffene Person für einen oder mehrere spezifische Zwecke der Verarbeitung (so genannte " Granularität " der Einwilligung[ii]) und des Grundsatzes der Zweckbestimmung zustimmt. Jeder der Zwecke der Datenverarbeitung muss von Anfang an klar definiert sein. Die betroffene Person sollte in der Lage sein zu entscheiden, für welche Zwecke sie zustimmen (z. B. Zustimmung für Zwecke A, B und C und nicht Zustimmung für Zweck E und D). Die Informationen im Zusammenhang mit der Einwilligung sollten eindeutig von Informationen in Bezug auf andere Angelegenheiten getrennt sein. Für jeden neuen Verarbeitungszweck muss eine Einwilligung eingeholt werden, und die für die Verarbeitung Verantwortlichen sollten mit jeder separaten Einwilligungserklärung spezifische Informationen über die Daten bereitstellen, die für jeden Zweck verarbeitet werden.
- "informiert" = Die Mindestanforderungen im Rahmen der Datenschutz-Grundverordnung umfassen die Bereitstellung von Informationen für den für die Verarbeitung Verantwortlichen und den Zweck der Verarbeitung. Die Artikel-29-Datenschutzgruppe (WP29) empfiehlt die Aufnahme zusätzlicher Informationen wie die Art der gesammelten und verwendeten Daten; das Recht, die Zustimmung zu widerrufen; Informationen über die Verwendung der Daten für Entscheidungen, die ausschließlich auf automatisierter Verarbeitung beruhen, einschließlich Profilerstellung[iii]; im Falle von Übermittlungen - Informationen über die möglichen Risiken von Datenübermittlungen in Drittstaaten in Ermangelung einer Angemessenheitsentscheidung und angemessener Garantien. [iv]
- "eindeutig" = Zustimmung muss durch eine Erklärung der betroffenen Person oder eine eindeutige zustimmende Handlung erteilt werden. Die Zustimmung muss immer durch einen aktiven Antrag oder eine Erklärung abgegeben werden. Daher können Schweigen, vorgestanzte Kästchen und Inaktivität keine gültige Zustimmung gemäß DSGVO darstellen;
- So leicht zurückgezogen wie gegeben = Zustimmung kann jederzeit widerrufen werden. Dies sollte nicht unbedingt mit derselben Aktion geschehen, aber der Prozess des Zurückziehens sollte so einfach sein wie der Prozess des Einverständnisses (z. B. das Anklicken eines Kästchens in der Online-Erklärung, um

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

die Gemeindezeitung zu erhalten, ist so einfach wie das Klicken auf einen Link in der E-Mail, die den Newsletter begleitet, um die Zustimmung zu widerrufen);

- Spezifische Anforderungen hinsichtlich der Einwilligung von Kindern = Die DSGVO behandelt Kinder als gefährdete Kategorie von Datensubjekten. Sie verdienen daher einen besonderen Schutz, da sie sich weniger der Risiken, Folgen und Garantien sowie ihrer Rechte in Bezug auf die Verarbeitung personenbezogener Daten bewusst sind. Im Falle der Bereitstellung von Diensten der Informationsgesellschaft für ein Kind (z. B. Online-Aufklärungskampagnen auf der Website der Gemeinden, die Erhebung von Kindern personenbezogene Daten erfordern), Zustimmung für die Verarbeitung von Kinderdaten unter 16 Jahren (die Mitgliedstaaten können dies senken Alter bis 13 Jahre) sollte vom Träger der elterlichen Verantwortung für das Kind erhalten oder genehmigt werden;
- Zustimmung gemäß Richtlinie 95/46 = Zustimmung, die bereits im Rahmen der alten Regelung eingeholt wurde, sollte nicht unbedingt überarbeitet werden müssen. Entspricht die Zustimmung den in der DSGVO festgelegten Anforderungen, sollte die nach der Richtlinie erlangte Zustimmung weiterhin als Grundlage für die Verarbeitung dienen.

Der Datenverantwortliche hat die Beweislast zu beweisen, dass die Einwilligung ordnungsgemäß eingeholt wurde. [v]

2.1.2. Anwendbarkeit im Rahmen der Tätigkeit der lokalen Behörden

In der Praxis wird die Zustimmung selten der grundlegende rechtliche Grund sein, auf dem die lokalen Behörden personenbezogene Daten von Bürgern rechtmäßig verarbeiten. Diese Schlussfolgerung ergibt sich aus den Anforderungen der DSGVO, die die Zustimmung erfüllen muss, um gültig zu sein.

Erstens sollte die Tatsache, dass die Einwilligung "frei gegeben" werden sollte, dh keine nachteiligen Folgen für die betroffene Person verursacht werden sollten, wenn keine Einwilligung gegeben wurde, bedeuten, dass in jeder Situation, in der bestimmte lokale Behörden als Inhaber öffentlicher Macht agieren, die Zustimmung erfolgen könnte nicht als gültige Rechtsgrundlage für die Verarbeitung verwendet werden. Die Kontrolle der ordnungsgemäßen Erfüllung der öffentlichen Pflichten der Bürger (z. B. Erhebung von lokalen Gebühren und Steuern, Registrierung des Erwerbs von Immobilien / Fahrzeugen usw.) und die Verhängung von Sanktionen im Falle der Nichterfüllung solcher

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

Verpflichtungen sind inhärent verbunden mit dem Recht (und die Pflicht), Zwangsgewalt auszuüben. Dies bedeutet, dass die betroffenen Personen keine echte freie Wahl haben, um der Verarbeitung ihrer personenbezogenen Daten zuzustimmen oder nicht. Sie sind untergeordnet und gesetzlich verpflichtet, mit lokalen Behörden zusammenzuarbeiten.

Zweitens könnte die Zustimmung "jederzeit" zurückgezogen werden. Wenn die Einwilligung der legitime Grund für die Verarbeitung personenbezogener Daten wäre, wenn Bürger ihren gesetzlichen Verpflichtungen nachkommen, könnte potentiell jeder Bürger, der bösgläubig handelt (z. B. nicht bereit ist, bestimmte öffentliche Verpflichtungen zu erfüllen), seine Zustimmung jederzeit widerrufen und diesen Widerruf verwenden Hindernisse (und in der Praxis "blockieren") das normale Funktionieren von lokaler Behörden zu schaffen. Wird die Einwilligung zurückgezogen, sollten lokale Behörden als Datenverantwortlicher die Verarbeitung beenden. Dies ist bei der Ausübung öffentlicher Gewalt undenkbar, da dies die gesamte Idee der Ausübung öffentlicher Macht gefährden würde.

Daher ist Zustimmung in den oben beschriebenen Situationen nicht das richtige Werkzeug für eine solche Verarbeitung.

Laut WP29 "ist die Verwendung der Einwilligung als rechtmäßige Grundlage für die Datenverarbeitung durch Behörden im Rechtsrahmen der DSGVO nicht völlig ausgeschlossen"[vi]. Daher kann die Einwilligung ein nützliches Werkzeug in Situationen sein, in denen lokale Behörden entweder ihre typischen und Hauptfunktionen nicht ausübt oder die entsprechende Verarbeitung eher fakultativ ist (und es werden standardmäßige Verarbeitungsprozeduren festgelegt, die stattfinden sollen, wenn die betroffene Person nicht zustimmt). Beispiele sind die folgenden Situationen:

- Lokale Behörden und Regierungsbehörden benötigen die gleichen Informationen für die Ausstellung eines bestimmten Rechtsakts auf Antrag eines Bürgers, können aber nicht auf die Datenbanken des anderen zugreifen. Da sie beide vom Bürger die gleichen Informationen verlangen, könnten sie die Zustimmung des Bürgers zur Zusammenführung der Dateien verlangen, um Doppelverfahren und Korrespondenz zu vermeiden. Beide öffentlichen Stellen sollten sicherstellen, dass dies optional ist und dass die Ausstellung des Dokuments auch dann gewährleistet wäre, wenn der Bürger der Zusammenlegung der Daten nicht zustimmt; [vii]
- Lokale Behörden sieht die Möglichkeit vor, die an einem Verwaltungsverfahren beteiligten Bürger per E-Mail darüber zu informieren. Das Regime ist opt-in, d.h. den Bürgern steht es frei zu entscheiden, ob sie per E-Mail benachrichtigt werden sollen (z. B. durch Ankreuzen des Kästchens in Online- / Papierform

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

verfügbar und ihre E-Mail-Adresse). Im Falle der Verweigerung der Zustimmung / Widerruf der Zustimmung, sollte die lokale Behörde ein Standardverfahren für die Benachrichtigung (z. B. per Einschreiben) haben. Die Bearbeitung der E-Mail würde in einem solchen Fall auf Einwilligung beruhen;

- Eine lokale Behörde bietet den Bürgern die Möglichkeit, Einladungen für verschiedene von lokalen Behörden organisierte Aktivitäten zu erhalten (z. B. Ausstellungen in lokalen Museen, Theaterpremieren im Gemeindetheater, Müllabfuhrkampagnen, Wettbewerbe / Aufklärungskampagnen in den Schulen der Gemeinde). Das Abonnement erfordert die Bereitstellung von Kontaktdaten (z. B. Postadresse, Telefonnummer, E-Mail usw.) sowie Daten für die Präferenzen der betroffenen Personen (z. B. Hobbys, Interessen usw.). Die Verarbeitung solcher Daten würde auf der Einwilligung beruhen, da die Bürger das Recht haben, sich jederzeit ohne Nachteil von solchen Mitteilungen abzumelden.

2.2. Erfüllung / Vertragsschluss mit der betroffenen Person

2.2.1. Bedeutung und rechtliche Anforderungen

Die Bestimmung von Artikel 6 Absatz 1 Buchstabe d der DSGVO führt zwei getrennte Rechtsgrundlagen für die Verarbeitung personenbezogener Daten ein:

(i) Situationen, in denen die Verarbeitung für die Erfüllung des Vertrags erforderlich ist, bei dem die betroffene Person Vertragspartei ist;

(ii) Situationen, in denen die Verarbeitung vor dem Abschluss eines Vertrags stattfindet. Dies gilt für vorvertragliche Beziehungen, sofern die Maßnahmen auf Wunsch der betroffenen Person und nicht auf Initiative des für die Verarbeitung Verantwortlichen oder eines Dritten ergriffen werden. [viii]

Die erste Hypothese sollte streng ausgelegt werden und sollte keine Situationen abdecken, in denen die Verarbeitung für die Erfüllung eines Vertrags nicht wirklich notwendig ist, sondern einseitig der betroffenen Person auferlegt wird.[ix] Nach der Auslegung der WP29 für den gleichen Grund nach der alten Richtlinie 95/46 gilt der genannte Rechtsgrund nur für das, was zur Erfüllung eines Vertrags erforderlich ist. Mit anderen Worten, solange die Verarbeitung die normale Ausführung eines Vertrags abdeckt, könnte sie in den genannten Rechtsgrund fallen. Dieser rechtliche Grund würde Situationen abdecken,

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

in denen die Verarbeitung im Rahmen eines Vertrags unabhängig von der jeweiligen Vertragsphase erfolgt. [x] Weitere Handlungen, die durch Nichteinhaltung oder alle anderen Vorfälle bei der Ausführung eines Vertrags ausgelöst werden, fallen jedoch nicht in den Anwendungsbereich dieses Rechtsgrundes. Solche Verarbeitungsarten erfordern die Anwendung unterschiedlicher rechtlicher Grundlagen - z.B. das berechtigte Interesse des für die Verarbeitung Verantwortlichen.

Die zweite Hypothese könnte die Verarbeitung umfassen, die für die Angebotserstellung, die Einstellung von Personalaktivitäten usw. erforderlich ist. Detaillierte Hintergrundüberprüfungen der Kandidaten wären jedoch ziemlich umfangreich und würden nicht als von der betroffenen Person angeforderte Schritte gerechtfertigt.

Im Allgemeinen wird dieser Rechtsgrund von den Regulierungsbehörden eng ausgelegt, so dass die für die Verarbeitung Verantwortlichen nachweisen können, dass die Verarbeitung unvermeidlich ist, um den Vertrag abzuschließen. [xi]

2.2.2. Anwendbarkeit im Rahmen der Tätigkeit der lokalen Behörden

Dieser rechtliche Grund für die Verarbeitung personenbezogener Daten könnte von den lokalen Behörden zumindest in folgenden Bereichen angewandt werden:

- Verarbeitung im Beschäftigungskontext - z.B. Verarbeitung von Gehaltsinformationen und Bankkontodetails, so dass Gehälter bezahlt werden können; [xii]
- Verarbeitung im Zusammenhang mit dem Abschluss von Verträgen für öffentliche Aufträge - dieser vertragliche Rechtsgrund könnte sich mit einem anderen Rechtsgrund für die Verarbeitung personenbezogener Daten überschneiden - z.B die gesetzliche Verpflichtung von lokalen Behörden zur Verarbeitung personenbezogener Daten im Rahmen des jeweiligen Verwaltungsverfahrens, das durch das lokale Recht auferlegt wird;
- Verarbeitung im Zusammenhang mit den Beziehungen zwischen einigen privaten Einrichtungen, die ganz oder teilweise Eigentum der Gemeinde / des Staates sind, und den Bürgern - z.B. Unternehmen, die öffentliche Verkehrsdienste in der gesamten Stadt / im Dorf anbieten, Unternehmen, die Versorgungsleistungen erbringen (Strom-, Gas-, Wasserversorgung usw.), wenn sie die entsprechenden Verträge abschließen.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

2.3. Rechtliche Verpflichtung

2.3.1. Bedeutung und rechtliche Anforderungen

Dieser rechtliche Grund erfordert eine klare gesetzliche Regelung, die entweder auf legislativer oder auf sublegislativer Ebene eingeführt wird (die in einigen Mitgliedstaaten als Sekundärrecht bezeichnete Stufe), die den für die Verarbeitung Verantwortlichen verpflichtet, die Verarbeitung durchzuführen. WP29 hebt hervor, dass das Gesetz alle relevanten Bedingungen erfüllen muss, um die Verpflichtung gültig und verbindlich zu machen, und dass es auch das Datenschutzrecht einschließlich des Erfordernisses der Notwendigkeit, Verhältnismäßigkeit und Zweckbindung einhalten muss[xiii]. Die DSGVO schreibt ausdrücklich vor, dass diese Verpflichtung kumulativ sein muss:

(i) eine Verpflichtung des Mitgliedstaats oder des Unionsrechts, der der für die Verarbeitung Verantwortliche unterliegt. Die WP29 hat in dieser Hinsicht bereits die alte Richtlinie 95/46 wie folgt ausgelegt: Verpflichtungen nach dem Recht von Drittländern (wie z. B. die Verpflichtung zur Einrichtung von Systemen zur Meldung von Missständen nach dem Sarbanes-Oxley Act von 2002 in den Vereinigten Staaten) fallen nicht unter die gesetzliche Grundpflicht. Um gültig zu sein, müsste eine rechtliche Verpflichtung eines Drittstaats amtlich anerkannt und in die Rechtsordnung des betreffenden Mitgliedstaats integriert werden, z.B. in Form eines internationalen Abkommens; und

(ii) "klar und präzise" und ihre Anwendung vorhersehbar für die davon Betroffenen sein muss. In den Erwägungsgründen 41 und 45 der DSGVO wird klargestellt, dass die maßgebliche "rechtliche Verpflichtung" nicht zwingend vorgeschrieben sein muss, was praktische Auswirkungen auf Staaten des Common Law haben könnte - es wäre ausreichend, wenn dies der "klaren und präzisen" Prüfung entspricht. Eine rechtliche Verpflichtung könnte sich auf mehrere Verarbeitungen erstrecken, die vom für die Verarbeitung Verantwortlichen durchgeführt werden, so dass es nicht erforderlich ist, für jede einzelne Verarbeitungstätigkeit eine spezifische rechtliche Verpflichtung zu ermitteln. [xiv]

WP29 hat darauf hingewiesen, dass der für die Verarbeitung Verantwortliche keine Wahl haben muss, ob er diese Verpflichtung auch erfüllen möchte. [xv] Freiwillige einseitige Verpflichtungen und öffentlich-private Partnerschaften, die Daten verarbeiten, die über die gesetzlichen Anforderungen hinausgehen, fallen somit nicht unter diesen rechtlichen Grund. . Die gesetzliche Verpflichtung als Grundlage für die Verarbeitung personenbezogener Daten sollte auf der Grundlage von Rechtsvorschriften gelten, die sich explizit auf die Art und den Zweck der Verarbeitung beziehen. Der für die Verarbeitung

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

Verantwortliche sollte keinen übermäßigen Ermessensspielraum bei der Erfüllung der gesetzlichen Verpflichtung haben. [xvi]

WP29 erkennt ausdrücklich an, dass die Gesetzgebung in einigen Fällen nur ein allgemeines Ziel festlegen kann, während spezifischere Verpflichtungen auf einer anderen Ebene auferlegt werden (z. B. im Sekundärrecht oder durch eine verbindliche Entscheidung einer Behörde). Nach WP29 kann dies auch zu rechtlichen Verpflichtungen führen, sofern Art und Zweck der Verarbeitung klar definiert sind und einer angemessenen Rechtsgrundlage unterliegen. [xvii]

2.3.2. Anwendbarkeit im Rahmen der Tätigkeit der örtlichen Behörden

In der Praxis wäre dieser rechtliche Grund einer der wichtigsten rechtlichen Gründe für die Verarbeitung personenbezogener Daten durch Gebietskörperschaften. Dieser rechtliche Grund würde sowohl Situationen abdecken, die mit der Erbringung von Verwaltungsdiensten verbunden sind, als auch die Erfüllung der öffentlichen Pflichten der Bürger erleichtern und bestimmte spezifische Verpflichtungen der lokalen Behörden in ihrer Eigenschaft als Arbeitgeber erfüllen. Dieser rechtliche Grund könnte z.B. in den folgenden Situationen:

- Sammlung von Daten durch lokale Behörden für die Behandlung von Strafen für das Parken an nicht autorisierten Orten;
- Meldung von Gehaltsdaten der lokalen Behörden Mitarbeiter an Sozialversicherungs- oder Steuerbehörden. [xviii]

2.4. Lebenswichtige Interessen

2.4.1. Bedeutung und rechtliche Anforderungen

Dieser rechtliche Grund ist sehr eng auszulegen. WP29 hat auch anerkannt, dass das lebenswichtige Interesse eine begrenzte Anwendung haben sollte. [xix] Der Begriff " lebenswichtiges Interesse" ist inhärent mit einer unmittelbaren Gefahr für grundlegende Güter der betroffenen Person (Leben, Gesundheit, Integrität des Körpers usw.) verbunden. In

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

der Rechtslehre wird darauf hingewiesen, dass die beabsichtigte Verarbeitung für das Überleben eines Individuums entscheidend sein sollte. [xx] Nach der Auslegung der WP29 nach der alten Richtlinie 95/46 sollte die Bedrohung unmittelbar erfolgen, d.h. Die Erhebung und Verarbeitung personenbezogener Daten in großem Umfang zu rein präventiven Zwecken könnte nicht in den Anwendungsbereich dieses Rechtsgrundes fallen. [xxi] Der 46. Erwägungsgrund der Datenschutz-Grundverordnung gestattet ausdrücklich die Verarbeitung auf diesem rechtlichen Grund für humanitäre Zwecke, einschließlich der Überwachung von Epidemien und deren Ausbreitung oder in Situationen humanitärer Notlagen, insbesondere in Situationen von Naturkatastrophen und von Menschen verursachten Katastrophen (in diesen Szenarien können sich beide überschneiden) die wichtigen Gründe des öffentlichen Interesses und das vitale Interesse). Daher könnte diese strenge Auslegung, die von der WP29 auferlegt wurde, in Zukunft "aufgeweicht" werden.

Es sei auch darauf hingewiesen, dass der Rechtsgrund "lebenswichtige Interessen" in der alten Richtlinie 95/46 nur das Interesse der betroffenen Person betraf. Mit der DSGVO wird der Geltungsbereich dieses rechtlichen Grundes erweitert - das wesentliche Interesse könnte entweder die betroffene Person oder eine andere natürliche Person sein. Die Datenschutz-Grundverordnung schreibt ausdrücklich vor, dass die Verarbeitung personenbezogener Daten, die auf den wesentlichen Interessen einer anderen natürlichen Person beruhen, grundsätzlich nur dann erfolgen sollte, wenn die Verarbeitung nicht offenkundig auf einer anderen Rechtsgrundlage beruhen kann. Mit anderen Worten, die Verarbeitung auf das lebenswichtige Interesse zu konzentrieren wäre eher eine "letzte Lösung" für die Controller.

2.4.2. Anwendbarkeit im Rahmen der Tätigkeit der örtlichen Behörden

Die Möglichkeit, diesen Hintergrund im Zusammenhang mit Aktivitäten lokaler Behörden anzuwenden, ist eher begrenzt. Dieser rechtliche Grund könnte theoretisch in einer sehr begrenzten Anzahl von Fällen angewendet werden, z.B. Prozessdaten personenbezogener Daten von Mitarbeitern oder Bürgern in Notfällen zu rechtfertigen, die innerhalb der Zuständigkeit der lokalen Behörde auftreten, und wenn es keinen anderen rechtlichen Grund für eine solche Verarbeitung gibt (z. B. gesetzliche Verpflichtung oder Ausübung hoheitlicher Befugnisse).

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

2.5. Aufgabe im öffentlichen Interesse

2.5.1. Bedeutung und rechtliche Anforderungen

Die Aufgabe oder die Befugnis des für die Verarbeitung Verantwortlichen sollte im Unionsrecht oder in den Rechtsvorschriften der Mitgliedstaaten festgelegt werden, denen der für die Verarbeitung Verantwortliche unterliegt. Aufgaben, die im öffentlichen Interesse eines Drittlandes oder in Ausübung einer nach ausländischem Recht gewährten Behörde durchgeführt werden, fallen nicht unter die alte Richtlinie 95/46[xxii] und dieser Ansatz wird mit der DSGVO fortgesetzt.

Das Analogon dieser Bestimmung im Rahmen der alten Richtlinie deckt zwei verschiedene Situationen ab:

i) wenn der für die Verarbeitung Verantwortliche selbst über eine amtliche Behörde oder eine Aufgabe von öffentlichem Interesse verfügt (aber nicht notwendigerweise verpflichtet ist, Daten zu verarbeiten) und die Verarbeitung für die Ausübung dieser Behörde oder die Wahrnehmung dieser Aufgabe erforderlich ist, oder

(ii) wenn der für die Verarbeitung Verantwortliche keine offizielle Behörde hat, aber von einem Dritten mit der Befugnis zur Offenlegung von Daten aufgefordert wird. [xxiii]

Die DSGVO hat das zweite Kriterium beseitigt, d. h. Situationen, in denen die Ausübung öffentlicher Gewalt einer Partei übertragen wurde, der die Daten mitgeteilt wurden, ist als Grundlage für die Datenverarbeitung nicht mehr relevant. [xxiv] Mit anderen Worten, die Umstände, in denen sich ein für die Verarbeitung Verantwortlicher auf diesen rechtlichen Grund stützen kann, sind enger als zuvor.

Die öffentliche Behörde oder öffentliche Aufgabe sollte in der Regel durch Gesetz oder andere gesetzliche Vorschriften zugewiesen werden. WP29 hat ausdrücklich eingeräumt, dass nach der DSGVO dieser rechtliche Grund so ausgelegt werden muss, dass die öffentlichen Behörden ein gewisses Maß an Flexibilität haben, um ihre ordnungsgemäße Verwaltung und Funktionsweise sicherzustellen. Daher sollten solche Aktivitäten nicht in den Anwendungsbereich dieses Rechtsgrundes fallen und könnte die Verarbeitung personenbezogener Daten auf dem berechtigten Interesse beruhen. [xxv]

Nicht zuletzt ist darauf hinzuweisen, dass die betroffenen Personen berechtigt sind, der Verarbeitung aufgrund dieses Rechtsgrundes zu widersprechen. Es liegt in der

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

Verantwortung des für die Verarbeitung Verantwortlichen, nachzuweisen, dass zwingende legitime Gründe für die Verarbeitung personenbezogener Daten vorliegen. [xxvi]

2.5.2. Anwendbarkeit im Rahmen der Tätigkeit der örtlichen Behörden

Zu den gesetzlichen Verpflichtungen nach Art. 6 Abs. 1, Punkt "c" der Datenschutz-Grundverordnung, wäre die im öffentlichen Interesse / Ausübung öffentlicher Gewalt ausgeübte Aufgabe einer der wichtigsten rechtlichen Gründe für die Tätigkeit der lokalen Behörden. Beispiele von WP29 für die Anwendung dieses Grundes sind:

- eine Steuerbehörde, die die Steuererklärung einer natürlichen Person sammelt und verarbeitet, um den zu entrichtenden Steuerbetrag festzustellen und zu überprüfen - analog könnte dieser Grund auch für lokale Gebietskörperschaften gelten, die lokale Steuern verwalten;
- eine lokale Regierungsbehörde (z. B. eine Gemeindebehörde), die mit der Aufgabe betraut ist, einen Bibliotheksdienst, eine Schule oder ein lokales Schwimmbad zu betreiben.

2.6. Legitime Interessen

2.6.1. Bedeutung und rechtliche Anforderungen

Der rechtliche Grund "legitime Interessen" umfasst zwei Elemente:

(i) Legitimes Interesse des für die Verarbeitung Verantwortlichen / Dritten:

ein.

a. Das Konzept des "Interesses" wird von der WP29 als eine breitere Beteiligung definiert, die ein für die Verarbeitung Verantwortlicher bei der Verarbeitung hat, oder für den Nutzen, den der Verantwortliche aus der Verarbeitung zieht - oder die die Gesellschaft möglicherweise herleiten könnte. [xxvii] Das Interesse könnte der Gesellschaft im Allgemeinen zugute kommen, könnte aber auch nur für den jeweiligen Datenverantwortlichen / Dritten von Vorteil sein;

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

b. Der Begriff der "Legitimität" ist inhärent mit der Einhaltung des Gesetzes verbunden - sowohl mit dem Datenschutzgesetz als auch mit den Gesetzen, die für die jeweilige Tätigkeit des für die Verarbeitung Verantwortlichen gelten. Mit anderen Worten, alle illegalen Ziele, die der für die Verarbeitung Verantwortliche / der Dritte verfolgt, würden die Anwendbarkeit dieses Rechtsgrundes ausschließen. In WP29 wurden die häufigsten Szenarien, in denen das berechtigte Interesse nach der alten Richtlinie 95/46 geltend gemacht werden könnte, nicht erschöpfend aufgelistet. Die Bereiche reichen von Werbe- / Aufmerksamkeitszwecken (z. B. Direktmarketing, Werbung oder unaufgeforderte nichtkommerzielle Botschaften, einschließlich für politische Kampagnen oder Sammeln von Spenden für Wohltätigkeitszwecke) zu gesellschaftlich nützlichen Aktivitäten (z. B. Hinweisspflichten, Ausübung des Rechts auf freie Meinungsäußerung) oder Information oder Verhinderung von Betrug, Missbrauch von Dienstleistungen oder Geldwäsche).

(ii) Das legitime Interesse sollte Vorrang vor den Interessen, Grundrechten und Grundfreiheiten haben und die betroffene Person = eine Abwägungsprüfung sollte von Fall zu Fall durchgeführt werden. Diese Anforderung ist inhärent mit dem Grundsatz der Verhältnismäßigkeit verbunden. Obwohl der für die Verarbeitung Verantwortliche / Dritte möglicherweise ein berechtigtes Interesse an der Durchführung der Verarbeitung haben, könnte dies unverhältnismäßig sein (z. B. könnte die jeweilige Verarbeitung zu aufdringlich sein, zu umfangreich, ohne angemessene Einschränkungen und Schutzmaßnahmen usw.) und in einem solchen Szenario die Verarbeitung wäre nicht als rechtmäßig gerechtfertigt. WP29 hat festgestellt, dass zu den Faktoren, die für den Ausgleichstest erforderlich sind, gehören:

a. Beurteilung des berechtigten Interesses des für die Verarbeitung Verantwortlichen;

b. Auswirkungen auf die betroffenen Personen;

c. vorläufiges Gleichgewicht und

d. zusätzliche Sicherheitsvorkehrungen, die der für die Verarbeitung Verantwortliche anwendet, um unzulässige Auswirkungen auf die betroffenen Personen zu verhindern. [xxviii]

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

2.6.2. Anwendbarkeit im Rahmen der Tätigkeit der örtlichen Behörden

Die DSGVO begrenzt die Anwendbarkeit des berechtigten Interesses im Zusammenhang mit den Tätigkeiten der Behörden erheblich. Die DSGVO sieht ausdrücklich vor, dass dieser Rechtsgrund nicht für die Verarbeitung gilt, die von öffentlichen Behörden bei der Erfüllung ihrer Aufgaben durchgeführt wird. Der Grund für diese Bestimmung ist, dass die öffentlichen Behörden gesetzlich dazu ermächtigt werden, ihre Aufgaben zu erfüllen.

Daher ist es für lokale Behörden, die sich auf legitimes Interesse verlassen, ratsam, ihre Aufgaben zu überdenken, welche anderen Rechtsgrundlagen für die Verarbeitung personenbezogener Daten sie anwenden könnten (z. B. Aufgabe im öffentlichen Interesse / Behörde).

Das legitime Interesse könnte jedoch von LA als legaler Boden für ihre internen Prozesse - z.B. in ihren HR-Aktivitäten.

3. SCHLUSSFOLGERUNG & PRAKTISCHE HINWEISE

Die Möglichkeit zu bestimmen, welcher rechtliche Grund für welche Verarbeitungstätigkeit gilt, ist für jeden für die Verarbeitung Verantwortlichen von wesentlicher Bedeutung, um die Rechtmäßigkeit der Verarbeitung zu gewährleisten. Darüber hinaus ist die Information, welcher Rechtsgrund für welchen Zweck der Verarbeitung gilt, eines der Schlüsselelemente des Transparenzgrundsatzes, da es ausdrücklich zu den Informationen gehört, die der für die Verarbeitung Verantwortliche jeder betroffenen Person zur Verfügung stellen muss (Art. 13 und Art. 14 der DSGVO). Daher sollten sowohl die öffentlichen als auch die privaten für die Verarbeitung Verantwortlichen die Bedeutung der einzelnen in Art. 6 der DSGVO. Die Verordnung sieht keine neuen rechtlichen Gründe vor, sondern ändert die Anforderungen und die Bedingungen für die Anwendbarkeit für einige der bestehenden Bestimmungen (z. B. Zustimmung, berechtigte Interessen). In jedem Fall ist es ein erster Schritt zur Gewährleistung der Einhaltung der DSGVO innerhalb der Organisation, die richtige rechtliche Grundlage zu finden. In der Doktrin wird darauf hingewiesen, dass ein umsichtiger Datenverantwortlicher die notwendigen Schritte unternehmen sollte, um zu gewährleisten, dass der für die Verarbeitung Verantwortliche in Fällen, in denen die Aufsichtsbehörde Nachweise benötigt, auf die Kriterien hinweisen kann, auf die er sich bei der Verarbeitung und der ordnungsgemäßen Notifizierung stützt die betroffenen Personen. [xxix]

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

4. EXTERNE QUELLEN & WEBLINKS

4.1. Bücher

- Voigt, P., von dem Bussche, A., The EU General Data Protection Regulation (GDPR) – A Practical Guide, Springer International Publishing (2017);
- Boardman, R., Mullock, J., Mole, A. Bird & Bird Guide to General Data Protection Regulation (2016);
- EU General Data Protection Regulation (GDPR). An Implementation and Compliance Guide, IT Governance Publishing, Cambridgeshire (2016);
- European Data Protection. Law and Practice, Executive Editor: Edurado Ustaran, CIPP/E, Partner, Hogan Lovells, IAPP (2018);

4.2. Dokumente der Artikel 29 Working Party

- WP29, Guidelines on Consent under Regulation 2016/679, WP 259;
- WP29, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, WP 217;

4.3. Web Links

- http://europa.eu/rapid/press-release_IP-18-386_en.htm
- https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en
- https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/grounds-processing/when-can-personal-data-be-processed_en
- https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/grounds-processing/what-does-grounds-legitimate-interest-mean_en
- https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/grounds-processing/when-consent-valid_en
- https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/grounds-processing/does-consent-given-25-may-2018-continue-be-valid-once-gdpr-starts-apply-25-may-2018_en

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

- https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/grounds-processing/what-if-somebody-withdraws-their-consent_en
- https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/grounds-processing/what-if-somebody-withdraws-their-consent_en

5. REFERENZEN

[i] WP29, Guidelines on Consent under Regulation 2016/679, WP 259, p. 6.
[ii] WP29, Guidelines on Consent under Regulation 2016/679, WP 259, p. 11-12.
[iii] More information on profiling is available in WP29 Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (project).
[iv] WP29, Guidelines on Consent under Regulation 2016/679, WP 259, p. 13.
[v] EU General Data Protection Regulation (GDPR). An Implementation and Compliance Guide, IT Governance Publishing, Cambridgeshire (2016), p. 189-190.
[vi] WP29, Guidelines on Consent under Regulation 2016/679, WP 259, p. 7.
[vii] The example is given in WP29, Guidelines on Consent under Regulation 2016/679, WP 259, p. 7.
[viii] WP29 Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, WP 217, p. 16-17.
[ix] Ibid, p. 16.
[x] Voigt, P., von dem Bussche, A., The EU General Data Protection Regulation (GDPR) – A Practical Guide, Springer International Publishing (2017), p. 102.
[xi] European Data Protection. Law and Practice, Executive Editor: Edurado Ustaran, CIPP/E, Partner, Hogan Lovells, IAPP (2018), p. 118
[xii] WP29 Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, WP 217, p. 16.
[xiii] Ibid, p. 20.
[xiv] Boardman, R., Mullock, J., Mole, A. Bird & Bird Guide to General Data Protection Regulation (2016), p. 10.
[xv] WP29 Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, WP 217, p. 19.
[xvi] Ibid, p. 19.
[xvii] Ibid, p. 20.
[xviii] Ibid, p. 19.
[xix] Ibid, p. 20.
[xx] European Data Protection. Law and Practice, Executive Editor: Edurado Ustaran, CIPP/E, Partner, Hogan Lovells, IAPP (2018), p. 119.
[xxi] WP29 Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, WP 217, p. 20-21.
[xxii] Ibid, p. 21.
[xxiii] Ibid, p. 21.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

[xxiv] European Data Protection. Law and Practice, Executive Editor: Edurado Ustaran, CIPP/E, Partner, Hogan Lovells, IAPP (2018), p. 119.
[xxv] WP29 Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, WP 217, p. 23.
[xxvi] European Data Protection. Law and Practice, Executive Editor: Edurado Ustaran, CIPP/E, Partner, Hogan Lovells, IAPP (2018), p. 119.
[xxvii] WP29 Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, WP 217, p. 24.
[xxviii] Ibid, p. 33.
[xxix] European Data Protection. Law and Practice, Executive Editor: Edurado Ustaran, CIPP/E, Partner, Hogan Lovells, IAPP (2018), p. 122.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

ProLegis

VERARBEITUNG SPEZIELLER KATEGORIEN VON PERSONENBEZOGENEN DATEN

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

Dissemination Level:		
PU	Public	
CO	Confidential, only for members of the consortium (including the Commission Services)	
EU-RES	Classified Information: RESTREINT UE (Commission Decision 2005/444/EC)	
EU-CON	Classified Information: CONFIDENTIEL UE (Commission Decision 2005/444/EC)	
EU-SEC	Classified Information: SECRET UE (Commission Decision 2005/444/EC)	
Document version control:		
Version	**Author(s)**	**Date**
Version 1	Developed by:	
Version 1	Reviewed & updated by:	
Version 2	Translated by: VICESSE	21/06/18

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

Inhaltsverzeichnis

1. RECHTLICHER RAHMEN 5

1.1. Charta der Grundrechte der EU 5

1.2. DSGVO 5

2. SPEZIELLE KATEGORIEN PERSÖNLICHE DATEN NACH DER DSGVO 11

2.1. Die Logik dahinter, bestimmte Kategorien von persönlichen Daten als speziell zu definieren 11

2.2. Arten von speziellen Kategorien persönlicher Daten 12

2.3. Personenbezogene Daten zu strafrechtlichen Verurteilungen und Straftaten 14

3. RECHTLICHE GRÜNDE FÜR DIE VERARBEITUNG BESONDERER KATEGORIEN PERSONENBEZOGENER DATEN 15

3.1. Ausdrückliche Zustimmung 15

3.2. Pflichten / besondere Rechte im Bereich des Beschäftigungs-, Sozialversicherungs- und Sozialschutzrechts 16

3.3. Lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person 17

3.4. Verarbeitung durch gemeinnützige Körperschaft mit einem politischen, philosophischen, religiösen oder gewerkschaftlichen Ziel 17

3.5. Die Daten werden offensichtlich von der betroffenen Person veröffentlicht 18

3.6. Begründung, Ausübung oder Verteidigung von Rechtsansprüchen / Gerichten, die in ihrer gerichtlichen Eigenschaft handeln 19

3.7. Erhebliches öffentliches Interesse auf der Grundlage des Rechts der EU oder der Mitgliedstaaten 19

3.8. Präventive oder Arbeitsmedizin, Beurteilung der Arbeitsfähigkeit des Arbeitnehmers, medizinische Diagnose, Bereitstellung von Gesundheits- oder Sozialpflege oder Behandlung 20

3.9. Öffentliches Interesse im Bereich der öffentlichen Gesundheit 20

3.10. Verarbeitung zu Archivierungszwecken im öffentlichen Interesse, zu wissenschaftlichen oder historischen Forschungszwecken oder zu statistischen Zwecken 21

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

3.11. Weitere Bedingungen in den Rechtsvorschriften der Mitgliedstaaten 21
4. ZUSAMMENFASSUNG & PRAKTISCHE TIPPS 21
5. EXTERNE QUELLEN & WEBLINKS 22
5.1. Bücher 22
5.2. Dokumente der Artikel 29 Working Party 22
5.3. Web Links 23
6. REFERENZEN 23

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

1. RECHTLICHER RAHMEN

1.1. Charta der Grundrechte der EU

Artikel 8

Schutz personenbezogener Daten

(1) Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten.

(2) Diese Daten dürfen nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der

betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet wer- den. Jede Person hat das Recht, Auskunft über die sie betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu erwirken.

(3) Die Einhaltung dieser Vorschriften wird von einer unabhängigen Stelle überwacht.

1.2. DSGVO

Artikel 4

Begriffsbestimmungen

Im Sinne dieser Verordnung bezeichnet der Ausdruck:

[…]

11. „Einwilligung“ der betroffenen Person jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist;

12. „Verletzung des Schutzes personenbezogener Daten“ eine Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden;

13. „genetische Daten“ personenbezogene Daten zu den ererbten oder erworbenen genetischen Eigenschaften einer natürlichen Person, die eindeutige Informationen über die Physiologie oder die Gesundheit dieser natürlichen Person liefern und insbesondere aus der Analyse einer biologischen Probe der betreffenden natürlichen Person gewonnen wurden;

Artikel 9

Verarbeitung besonderer Kategorien personenbezogener Daten

(1) Die Verarbeitung personenbezogener Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person ist untersagt.

(2) Absatz 1 gilt nicht in folgenden Fällen:

a) Die betroffene Person hat in die Verarbeitung der genannten personenbezogenen Daten für einen oder mehrere festgelegte Zwecke ausdrücklich eingewilligt, es sei denn, nach Unionsrecht oder dem Recht der Mitgliedstaaten kann das Verbot nach Absatz 1 durch die Einwilligung der betroffenen Person nicht aufgehoben werden,

b) die Verarbeitung ist erforderlich, damit der Verantwortliche oder die betroffene Person die ihm bzw. ihr aus dem Arbeitsrecht und dem Recht der sozialen Sicherheit und des Sozialschutzes erwachsenden Rechte ausüben und seinen bzw. ihren diesbezüglichen Pflichten nachkommen kann, soweit dies nach Unionsrecht oder dem Recht der Mitgliedstaaten oder einer Kollektivvereinbarung nach dem Recht der Mitgliedstaaten, das geeignete Garantien für die Grundrechte und die Interessen der betroffenen Person vorsieht, zulässig ist,

c) die Verarbeitung ist zum Schutz lebenswichtiger Interessen der betroffenen Person oder einer anderen natürlichen Person erforderlich und die betroffene Person ist aus körperlichen oder rechtlichen Gründen außerstande, ihre Einwilligung zu geben,

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

d) die Verarbeitung erfolgt auf der Grundlage geeigneter Garantien durch eine politisch, weltanschaulich, religiös oder gewerkschaftlich ausgerichtete Stiftung, Vereinigung oder sonstige Organisation ohne Gewinnerzielungsabsicht im Rahmen ihrer rechtmäßigen Tätigkeiten und unter der Voraussetzung, dass sich die Verarbeitung ausschließlich auf die Mitglieder oder ehemalige Mitglieder der Organisation oder auf Personen, die im Zusammenhang mit deren Tätigkeitszweck regelmäßige Kontakte mit ihr unterhalten, bezieht und die personenbezogenen Daten nicht ohne Einwilligung der betroffenen Personen nach außen offengelegt werden,

e) die Verarbeitung bezieht sich auf personenbezogene Daten, die die betroffene Person offensichtlich öffentlich gemacht hat,

f) die Verarbeitung ist zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen oder bei Handlungen der Gerichte im Rahmen ihrer justiziellen Tätigkeit erforderlich,

g) die Verarbeitung ist auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats, das in angemessenem Verhältnis zu dem verfolgten Ziel steht, den Wesensgehalt des Rechts auf Datenschutz wahrt und angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person vorsieht, aus Gründen eines erheblichen öffentlichen Interesses erforderlich,

h) die Verarbeitung ist für Zwecke der Gesundheitsvorsorge oder der Arbeitsmedizin, für die Beurteilung der Arbeitsfähigkeit des Beschäftigten, für die medizinische Diagnostik, die Versorgung oder Behandlung im Gesundheits- oder Sozialbereich oder für die Verwaltung von Systemen und Diensten im Gesundheits- oder Sozialbereich auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats oder aufgrund eines Vertrags mit einem Angehörigen eines Gesundheitsberufs und vorbehaltlich der in Absatz 3 genannten Bedingungen und Garantien erforderlich,

i) die Verarbeitung ist aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit, wie dem Schutz vor schwerwiegenden grenzüberschreitenden Gesundheitsgefahren oder zur Gewährleistung hoher Qualitäts- und Sicherheitsstandards bei der Gesundheitsversorgung und bei Arzneimitteln und Medizinprodukten, auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats, das angemessene und spezifische Maßnahmen zur Wahrung der Rechte und Freiheiten der betroffenen Person, insbesondere des Berufsgeheimnisses, vorsieht, erforderlich, oder

j) die Verarbeitung ist auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats, das in angemessenem Verhältnis zu dem verfolgten Ziel steht, den

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

Wesensgehalt des Rechts auf Datenschutz wahrt und angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person vorsieht, für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gemäß Artikel 89 Absatz 1 erforderlich.

(3) Die in Absatz 1 genannten personenbezogenen Daten dürfen zu den in Absatz 2 Buchstabe h genannten Zwecken verarbeitet werden, wenn diese Daten von Fachpersonal oder unter dessen Verantwortung verarbeitet werden und dieses Fachpersonal nach dem Unionsrecht oder dem Recht eines Mitgliedstaats oder den Vorschriften nationaler zuständiger Stellen dem Berufsgeheimnis unterliegt, oder wenn die Verarbeitung durch eine andere Person erfolgt, die ebenfalls nach dem Unionsrecht oder dem Recht eines Mitgliedstaats oder den Vorschriften nationaler zuständiger Stellen einer Geheimhaltungspflicht unterliegt.

(4) Die Mitgliedstaaten können zusätzliche Bedingungen, einschließlich Beschränkungen, einführen oder aufrechterhalten, soweit die Verarbeitung von genetischen, biometrischen oder Gesundheitsdaten betroffen ist.

Artikel 10

Verarbeitung von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten

Die Verarbeitung personenbezogener Daten über strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherungsmaßregeln aufgrund von Artikel 6 Absatz 1 darf nur unter behördlicher Aufsicht vorgenommen werden oder wenn dies nach dem Unionsrecht oder dem Recht der Mitgliedstaaten, das geeignete Garantien für die Rechte und Freiheiten der betroffenen Personen vorsieht, zulässig ist. Ein umfassendes Register der strafrechtlichen Verurteilungen darf nur unter behördlicher Aufsicht geführt werden.

Erwägungsgründe

(51) Personenbezogene Daten, die ihrem Wesen nach hinsichtlich der Grundrechte und Grundfreiheiten besonders sensibel sind, verdienen einen besonderen Schutz, da im Zusammenhang mit ihrer Verarbeitung erhebliche Risiken für die Grundrechte und

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

Grundfreiheiten auftreten können. Diese personenbezogenen Daten sollten personenbezogene Daten umfassen, aus denen die rassische oder ethnische Herkunft hervorgeht, wobei die Verwendung des Begriffs „rassische Herkunft“ in dieser Verordnung nicht bedeutet, dass die Union Theorien, mit denen versucht wird, die Existenz verschiedener menschlicher Rassen zu belegen, gutheißt. Die Verarbeitung von Lichtbildern sollte nicht grundsätzlich als Verarbeitung besonderer Kategorien von personenbezogenen Daten angesehen werden, da Lichtbilder nur dann von der Definition des Begriffs „biometrische Daten“ erfasst werden, wenn sie mit speziellen technischen Mitteln verarbeitet werden, die die eindeutige Identifizierung oder Authentifizierung einer natürlichen Person ermöglichen. Derartige personenbezogene Daten sollten nicht verarbeitet werden, es sei denn, die Verarbeitung ist in den in dieser Verordnung dargelegten besonderen Fällen zulässig, wobei zu berücksichtigen ist, dass im Recht der Mitgliedstaaten besondere Datenschutzbestimmungen festgelegt sein können, um die Anwendung der Bestimmungen dieser Verordnung anzupassen, damit die Einhaltung einer rechtlichen Verpflichtung oder die Wahrnehmung einer Aufgabe im öffentlichen Interesse oder die Ausübung öffentlicher Gewalt, die dem Verantwortlichen übertragen wurde, möglich ist. Zusätzlich zu den speziellen Anforderungen an eine derartige Verarbeitung sollten die allgemeinen Grundsätze und andere Bestimmungen dieser Verordnung, insbesondere hinsichtlich der Bedingungen für eine rechtmäßige Verarbeitung, gelten. Ausnahmen von dem allgemeinen Verbot der Verarbeitung dieser besonderen Kategorien personenbezogener Daten sollten ausdrücklich vorgesehen werden, unter anderem bei ausdrücklicher Einwilligung der betroffenen Person oder bei bestimmten Notwendigkeiten, insbesondere wenn die Verarbeitung im Rahmen rechtmäßiger Tätigkeiten bestimmter Vereinigungen oder Stiftungen vorgenommen wird, die sich für die Ausübung von Grundfreiheiten einsetzen.

(52) Ausnahmen vom Verbot der Verarbeitung besonderer Kategorien von personenbezogenen Daten sollten auch erlaubt sein, wenn sie im Unionsrecht oder dem Recht der Mitgliedstaaten vorgesehen sind, und — vorbehaltlich angemessener Garantien zum Schutz der personenbezogenen Daten und anderer Grundrechte — wenn dies durch das öffentliche Interesse gerechtfertigt ist, insbesondere für die Verarbeitung von personenbezogenen Daten auf dem Gebiet des Arbeitsrechts und des Rechts der sozialen Sicherheit einschließlich Renten und zwecks Sicherstellung und Überwachung der Gesundheit und Gesundheitswarnungen, Prävention oder Kontrolle ansteckender Krankheiten und anderer schwerwiegender Gesundheitsgefahren. Eine solche Ausnahme kann zu gesundheitlichen Zwecken gemacht werden, wie der Gewährleistung der öffentlichen Gesundheit und der Verwaltung von Leistungen der Gesundheitsversorgung, insbesondere wenn dadurch die Qualität und Wirtschaftlichkeit der Verfahren zur Abrechnung von Leistungen in den sozialen Krankenversicherungssystemen sichergestellt werden soll, oder

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

wenn die Verarbeitung im öffentlichen Interesse liegenden Archivzwecken, wissenschaftlichen oder historischen Forschungszwecken oder statistischen Zwecken dient. Die Verarbeitung solcher personenbezogener Daten sollte zudem ausnahmsweise erlaubt sein, wenn sie erforderlich ist, um rechtliche Ansprüche, sei es in einem Gerichtsverfahren oder in einem Verwaltungsverfahren oder einem außergerichtlichen Verfahren, geltend zu machen, auszuüben oder zu verteidigen.

(53) Besondere Kategorien personenbezogener Daten, die eines höheren Schutzes verdienen, sollten nur dann für gesundheitsbezogene Zwecke verarbeitet werden, wenn dies für das Erreichen dieser Zwecke im Interesse einzelner natürlicher Personen und der Gesellschaft insgesamt erforderlich ist, insbesondere im Zusammenhang mit der Verwaltung der Dienste und Systeme des Gesundheits- oder Sozialbereichs, einschließlich der Verarbeitung dieser Daten durch die Verwaltung und die zentralen nationalen Gesundheitsbehörden zwecks Qualitätskontrolle, Verwaltungsinformationen und der allgemeinen nationalen und lokalen Überwachung des Gesundheitssystems oder des Sozialsystems und zwecks Gewährleistung der Kontinuität der Gesundheits- und Sozialfürsorge und der grenzüberschreitenden Gesundheitsversorgung oder Sicherstellung und Überwachung der Gesundheit und Gesundheitswarnungen oder für im öffentlichen Interesse liegende Archivzwecke, zu wissenschaftlichen oder historischen Forschungszwecken oder statistischen Zwecken, die auf Rechtsvorschriften der Union oder der Mitgliedstaaten beruhen, die einem im öffentlichen Interesse liegenden Ziel dienen müssen, sowie für Studien, die im öffentlichen Interesse im Bereich der öffentlichen Gesundheit durchgeführt werden. Diese Verordnung sollte daher harmonisierte Bedingungen für die Verarbeitung besonderer Kategorien personenbezogener Gesundheitsdaten im Hinblick auf bestimmte Erfordernisse harmonisieren, insbesondere wenn die Verarbeitung dieser Daten für gesundheitsbezogene Zwecke von Personen durchgeführt wird, die gemäß einer rechtlichen Verpflichtung dem Berufsgeheimnis unterliegen. Im Recht der Union oder der Mitgliedstaaten sollten besondere und angemessene Maßnahmen zum Schutz der Grundrechte und der personenbezogenen Daten natürlicher Personen vorgesehen werden. Den Mitgliedstaaten sollte gestattet werden, weitere Bedingungen — einschließlich Beschränkungen — in Bezug auf die Verarbeitung von genetischen Daten, biometrischen Daten oder Gesundheitsdaten beizubehalten oder einzuführen. Dies sollte jedoch den freien Verkehr personenbezogener Daten innerhalb der Union nicht beeinträchtigen, falls die betreffenden Bedingungen für die grenzüberschreitende Verarbeitung solcher Daten gelten.

(54) Aus Gründen des öffentlichen Interesses in Bereichen der öffentlichen Gesundheit kann es notwendig sein, besondere Kategorien personenbezogener Daten auch ohne Einwilligung der betroffenen Person zu verarbeiten. Diese Verarbeitung sollte

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

angemessenen und besonderen Maßnahmen zum Schutz der Rechte und Freiheiten natürlicher Personen unterliegen. In diesem Zusammenhang sollte der Begriff „öffentliche Gesundheit“ im Sinne der Verordnung (EG) Nr. 1338/2008 des Europäischen Parlaments und des Rates (11) ausgelegt werden und alle Elemente im Zusammenhang mit der Gesundheit wie den Gesundheitszustand einschließlich Morbidität und Behinderung, die sich auf diesen Gesundheitszustand auswirkenden Determinanten, den Bedarf an Gesundheitsversorgung, die der Gesundheitsversorgung zugewiesenen Mittel, die Bereitstellung von Gesundheitsversorgungsleistungen und den allgemeinen Zugang zu diesen Leistungen sowie die entsprechenden Ausgaben und die Finanzierung und schließlich die Ursachen der Mortalität einschließen. Eine solche Verarbeitung von Gesundheitsdaten aus Gründen des öffentlichen Interesses darf nicht dazu führen, dass Dritte, unter anderem Arbeitgeber oder Versicherungs- und Finanzunternehmen, solche personenbezogene Daten zu anderen Zwecken verarbeiten.

(55) Auch die Verarbeitung personenbezogener Daten durch staatliche Stellen zu verfassungsrechtlich oder völkerrechtlich verankerten Zielen von staatlich anerkannten Religionsgemeinschaften erfolgt aus Gründen des öffentlichen Interesses.

(56) Wenn es in einem Mitgliedstaat das Funktionieren des demokratischen Systems erfordert, dass die politischen Parteien im Zusammenhang mit Wahlen personenbezogene Daten über die politische Einstellung von Personen sammeln, kann die Verarbeitung derartiger Daten aus Gründen des öffentlichen Interesses zugelassen werden, sofern geeignete Garantien vorgesehen werden.

2. SPEZIELLE KATEGORIEN PERSÖNLICHE DATEN NACH DER DSGVO

2.1. Die Logik dahinter, bestimmte Kategorien von persönlichen Daten als speziell zu definieren

Bereits im Zuge der Ausarbeitung des ersten EU-Rechtsakts zum Schutz personenbezogener Daten - der Richtlinie 95/46 - hat die Europäische Kommission hervorgehoben, dass die Verarbeitung bestimmter Kategorien personenbezogener Daten ein höheres Risiko für die Grundrechte und -freiheiten der europäischen Bürger bedeuten könnte[i]. Daher wurde ein allgemeines Verbot für die Verarbeitung solcher "riskanten" Kategorien personenbezogener Daten eingeführt. Sie wurden "besondere Kategorien

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

personenbezogener Daten" genannt, aber in der Praxis wurden sie aufgrund ihrer sensiblen Natur für die Privatsphäre des Einzelnen auch als "sensible Daten" bezeichnet[ii]. Diese Daten könnten nur in Ausnahmefällen verarbeitet werden, die erschöpfend in den Datenschutzvorschriften der Mitgliedstaaten aufgeführt sind.

Die DSGVO setzt diesen Ansatz fort, erweitert jedoch den Anwendungsbereich der besonderen Kategorien personenbezogener Daten und sieht einige neue Ausnahmen vor (rechtliche Gründe), die den für die Verarbeitung Verantwortlichen zur Verarbeitung solcher Daten berechtigen.

Es sollte erwähnt werden, dass verschiedene Arten von Daten unterschiedliche Auswirkungen auf die Individuen haben. Welche Daten als sensibel definiert sind, basiert auf einem objektiven und nicht auf einem subjektiven Prinzip. Mit anderen Worten, jemand könnte das Gefühl haben, dass die Daten bezüglich ihres finanziellen Status, der Geschichte der Disziplinarstrafen oder der Eindeutigen Identifikationsnummer / Sozialversicherungsnummer sensibel sind. Wenn solche Daten vom europäischen Gesetzgeber jedoch nicht als sensibel anerkannt werden, würden sie nicht unter die Sonderregelung für die Verarbeitung solcher Daten fallen, unabhängig von ihrer subjektiven Empfindlichkeit.

In der Doktrin wird darauf hingewiesen, dass die Auswahl der Kategorien von persönlichen Daten, die als besonders definiert werden, wesentlich durch Antidiskriminierungsgesetze beeinflusst wurde, weshalb Daten wie Sozialversicherungsnummern und Kreditkartendetails (die bei Missbrauch einen ernsthaften Schaden verursachen könnten) erklärt werden zu den Individuen) sind nicht als sensibel definiert[iii].

2.2. Arten von speziellen Kategorien persönlicher Daten

Nach Art. 9, Abs. 1 der Datenschutz-Grundverordnung, die folgenden Arten von personenbezogenen Daten sind besondere Kategorie (sensible Daten):

- **Personenbezogene Daten, aus denen die ethnische Herkunft hervorgeht** = Diese Kategorien personenbezogener Daten werden als sensibel definiert, da sie ein hohes Risiko der Diskriminierung beinhalten. In der Rechtslehre werden die folgenden Beispiele gegeben, welche Daten in diese Kategorie fallen könnten: Vorname und Nachname der Person, Geburtsort, Muttersprache oder die Namen seiner Eltern, die, wenn sie kombiniert werden, Rückschlüsse auf seine Herkunft;

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

- **Politische Meinungen** = diese Daten verdienen einen besonderen Schutz, weil sie mit der Garantie der Bürger verbunden sind, Meinungen über die Politik zu bilden und letztlich (aktiv als Politiker und / oder passiv als Wähler und Mitglieder der Zivilgesellschaft) am politischen Leben teilzunehmen das Land. Beispiele für solche Daten sind Informationen über die Mitgliedschaft in einer politischen Partei, Informationen über den Beitritt zu Petitionen, die Teilnahme an Demonstrationen, politische Treffen oder ähnliche Veranstaltungen, Informationen über die Unterstützung einer bestimmten politischen Idee oder deren Ablehnung
- **Religiöse oder philosophische Überzeugungen** = Diese Kategorien von Daten sind eng mit der Gewissensfreiheit verbunden, d. H. Der Freiheit zu entscheiden, ob wir an transzendente Kräfte glauben sollen, die unser tägliches Leben vorgeben und ob wir es manifestieren oder nicht. Die Geschichte der Menschheit ist voll von Beispielen, wo Gewalt aufgrund religiöser Unterschiede stattgefunden hat, daher sollten solche Daten auch im Rahmen der Datenschutzgesetze besonders geschützt werden;
- **Gewerkschaftsmitgliedschaft** = Informationen über solche Mitgliedschaften sind heikel, weil dadurch das Risiko einer diskriminierenden Behandlung im Bereich des Arbeitsrechts besteht. Die europäischen Bürger haben die Freiheit zu Kollektivverhandlungen und Handeln und sollten daher nicht auf der Grundlage ihrer Gewerkschaftszugehörigkeit ungleich behandelt werden[iv];
- **Genetische Daten** = neue Kategorie, die von der DSGVO als sensible Daten eingeführt wurde. Die DSGVO definiert sie als "Daten in Bezug auf die ererbten oder erworbenen genetischen Merkmale einer natürlichen Person, die eindeutige Informationen über die Physiologie der natürlichen Person liefern und insbesondere in Frage kommen". Einige Mitgliedstaaten haben bereits den Status, für diese Art von Daten[v] sensibel zu sein, aber die DSGVO führt sie erstmals auf EU-Ebene ein. Genetische Daten sollten geschützt werden, da sich solche Daten nicht nur auf die betroffene Person beziehen, sondern potenziell auch einen undefinierten Kreis von Personen betreffen können, die Teil des Stammbaums der Person sind (einschließlich Daten von Todesopfern, Daten von Kindern usw.). Darüber hinaus könnte die detaillierte Analyse solcher Daten andere Arten von sensiblen Informationen wie psychologische Daten oder Gesundheitsdaten (z. B. Prädisposition für Krankheiten, Vulnerabilität usw.);
- **Biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person =** Diese Arten von Daten verdienen Schutz, weil sie es den Kontrolleuren ermöglichen, eine bestimmte natürliche Person aufgrund ihrer physischen oder Verhaltensmerkmale eindeutig zu identifizieren: Fingerabdrücke, Gesichtserkennung, Iris, Netzhaut, Gefäßmodelle, DNA, Sprache, Unterschrift,

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

Tastaturinteraktion , etc.). Da die Verarbeitung solcher Arten von Daten mit der Einführung verschiedener technologischer Entscheidungen (z. B. Systeme für die Zugangskontrolle zu Räumlichkeiten, Systeme zur Identifikation auf entfernten Geräten wie Mobiltelefonen, Tablets usw.) immer häufiger wird, sollte eine solche Verarbeitung erfolgen restriktiver und kontrollierter, und diese Faktoren rechtfertigen die Aufnahme dieser Daten in die Liste der "sensiblen" Daten im Rahmen der DSGVO. Im Gegensatz zu den in einigen Mitgliedstaaten praktizierten Praktiken wird die Verarbeitung von Fotos nicht automatisch als sensible Verarbeitung angesehen. Fotografien werden nur dann als sensible Daten angesehen, wenn sie die eindeutige Identifizierung oder Authentifizierung einer Person als biometrisch ermöglichen (z. B. in einem elektronischen Reisepass oder einer anderen Art von Ausweisdokumenten)[vi];

- **Daten über Gesundheit oder Daten über das Sexualleben oder die sexuelle Orientierung einer natürlichen Person** = Solche Daten sind sehr sensibel, da sie in die intimsten Aspekte des Lebens des Individuums eingreifen. Darüber hinaus birgt die Information in Bezug auf Sexualleben und sexuelle Orientierung die Gefahr von Diskriminierung, Manipulation usw. In der Theorie wird darauf hingewiesen, dass diese Daten auch die genaue Identität der Partner einer Person enthalten.[vii]

2.3. Personenbezogene Daten zu strafrechtlichen Verurteilungen und Straftaten

Personenbezogene Daten in Bezug auf strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherheitsmaßnahmen werden nicht als besondere Kategorie personenbezogener Daten ausgerufen. Die Gesetzgebung einiger Mitgliedstaaten behandelt sie jedoch als sensibel. Diese Art von Informationen birgt jedoch auch das Risiko einer Ungleichbehandlung (z. B. im Bereich der Beschäftigung), so dass diese Daten auch besonderen Regeln für die Verarbeitung unterliegen. Die DSGVO führt gegenüber der alten Richtlinie 95/46 in Bezug auf Daten zu strafrechtlichen Verurteilungen und Straftaten keine wesentlichen Änderungen ein. Angesichts der Tatsache, dass die Vorschriften der Richtlinie in den Mitgliedstaaten unterschiedlich umgesetzt wurden, würde die DSGVO gleichzeitig einen allgemeineren Ansatz auf EU-Ebene in Bezug auf solche Daten einführen. Nach dem Wortlaut des Art. 10 der DSGVO könnten diese Daten auf der Grundlage eines der in Art. 6 vorausgesetzt, dass eine von zwei alternativen zusätzlichen Bedingungen erfüllt ist:

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

(i) die Verarbeitung sollte unter der Kontrolle der Behörde stehen, oder
(ii) Die Verarbeitung ist nach dem Recht der EU / Mitgliedstaaten zulässig, das angemessene Garantien für die Rechte und Freiheiten der betroffenen Personen vorsieht.

Diese Bestimmung ist mit Unsicherheiten behaftet, da nicht klar ist, wie diese beiden zusätzlichen Anforderungen in Verbindung mit Art. 6 auszulegen sind. Die konservative Auslegung besagt, dass private oder gewerbliche Einrichtungen solche Daten nicht verarbeiten könnten, mit anderen Worten: "In der Verordnung ist kein Platz für die private oder kommerzielle Verarbeitung dieser Daten".[viii] Die andere Interpretation ist, dass diese Art von Daten unter allen möglichen rechtlichen Gründen verarbeitet werden könnten, vorausgesetzt, dass die zusätzlichen Bedingungen (unter der Kontrolle der offiziellen Behörde oder wenn dies nach dem anwendbaren Recht zulässig ist) erfüllt sind. In der Doktrin wird darauf hingewiesen, dass diese Bestimmung wahrscheinlich zu einer anhaltenden nationalen Divergenz führen würde. Obwohl die lokalen Behörden als öffentliche Behörden fungieren und theoretisch die erste zusätzliche Verarbeitungsanforderung (unter der Kontrolle der Behörde) rechtfertigen könnten, wäre es dennoch ratsam, die lokalen Vorschriften sorgfältig zu prüfen, wenn solche Arten von Daten verarbeitet werden könnten (insbesondere im Zusammenhang mit HR-Aktivitäten und der Erhebung von Strafregister, da die jeweilige Behörde in diesem Kontext eher als Arbeitgeber fungiert als als öffentlicher Machtträger und die Anwendbarkeit der ersten zusätzlichen Bedingung fraglich ist).

3. RECHTLICHE GRÜNDE FÜR DIE VERARBEITUNG BESONDERER KATEGORIEN PERSONENBEZOGENER DATEN

Das generelle Verbot der Verarbeitung besonderer Kategorien personenbezogener Daten gilt nicht, sofern eine der folgenden alternativen Bedingungen erfüllt ist:

3.1. Ausdrückliche Zustimmung

Die Anforderungen, die im Rahmen der DSGVO zu erfüllen sind, um eine gültige Zustimmung zu haben (frei gegeben, spezifisch, informiert, eindeutig), gelten in jedem Fall für die Verarbeitung personenbezogener Daten bestimmter Kategorien. Das Element "explizit" ist in der DSGVO nicht definiert. Die Artikel-29-Datenschutzgruppe (WP29) hat darauf hingewiesen, dass eine ausdrückliche Zustimmung in Situationen erforderlich ist, in

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

denen ein ernsthaftes Datenschutzrisiko besteht, und dass ein hohes Maß an individueller Kontrolle personenbezogener Daten angemessen ist.

Der Begriff "explizit" bezieht sich auf die Art und Weise, wie die betroffene Person die Einwilligung ausspricht - die betroffene Person muss eine ausdrückliche Einverständniserklärung abgeben. Eine Möglichkeit zur Einwilligung besteht darin, dies ausdrücklich schriftlich zu bestätigen. Im Online-Kontext können verschiedene Lösungen durch Ausfüllen eines elektronischen Formulars, Senden einer E-Mail, Hochladen eines gescannten Dokuments mit der Unterschrift der betroffenen Person oder durch Verwendung einer elektronischen Signatur angewendet werden. Alle anderen Mittel, die es dem für die Verarbeitung Verantwortlichen ermöglichen würden, die hohe Schwelle für die Art der Erteilung der Zustimmung nachzuweisen, wären angemessen.

Angesichts der Unausgewogenheit der Befugnisse zwischen den betroffenen Personen und den Behörden ist es nicht ratsam, dass sich die lokalen Behörden überwiegend auf die ausdrückliche Zustimmung zur Verarbeitung besonderer Kategorien personenbezogener Daten (auch in den Beziehungen zu Bürgern und Arbeitnehmern) stützen.

3.2. Pflichten / besondere Rechte im Bereich des Beschäftigungs-, Sozialversicherungs- und Sozialschutzrechts

Diese Bedingung ist besonders relevant für LAs bei der Verwaltung ihres internen HR-Prozesses. Die Verarbeitung besonderer Kategorien personenbezogener Daten könnte in jeder Phase des Arbeitsverhältnisses erforderlich sein - von der Entstehung (Einstellung neuer Mitarbeiter) über die Durchführung und Änderung bis hin zur Beendigung des Arbeitsverhältnisses.

Beispiele, bei denen eine solche Verarbeitung erforderlich sein könnte, umfassen die Verwaltung von Krankenblättern und Mutterschaftsurlaub; Überstellung des Arbeitnehmers aus Gesundheitsgründen auf Antrag der Gesundheitsbehörden an eine geeignetere Stelle; Einhaltung zwingender Regeln, die einen besonderen Schutz bestimmter Kategorien von Arbeitnehmern bei Beendigung des Arbeitsverhältnisses vorsehen, usw.

Die allgemeinen Anforderungen, die in der DSGVO für die Anwendung dieses Grundes eingeführt wurden, sind:

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

(i) Die Verarbeitung muss notwendig sein, um eine Verpflichtung des für die Verarbeitung Verantwortlichen oder ein bestimmtes Recht der betroffenen Person zu erfüllen;
(ii) Diese Verpflichtung / dieses Recht könnte im Recht der EU / des Mitgliedstaates oder in einer Kollektivvereinbarung (Verhandlungsvereinbarung) vorgesehen werden;

Es sollte angemessene Garantien für die Grundrechte und die Interessen der betroffenen Person geben.

Um diesen rechtlichen Grund zu nutzen, müssen die spezifischen nationalen Rechtsvorschriften im jeweiligen Mitgliedstaat, in dem das LA als Arbeitgeber tätig ist, beachtet werden. Da das Arbeitsgesetz zu den Bereichen gehört, in denen die DSGVO die Mitgliedstaaten ermächtigt, zusätzliche Rechtsvorschriften im Bereich des Schutzes personenbezogener Daten zu erlassen (Artikel 88), empfiehlt sich bei der Anwendung dieses Grundes ein lokales Konzept für Gebietskörperschaften.

3.3. Lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person

Ähnlich dem Rechtsgrund unter Art. 6, Abs. 1, Punkt "d" der DSGVO, bezieht sich diese Situation auf Lebens- oder Todesumstände. Das wesentliche Interesse könnte entweder die betroffene Person oder eine andere Person sein. Was ist anders im Vergleich zu Art. 6 ist, dass der für die Verarbeitung Verantwortliche die Beweislast für das Vorliegen einer zusätzlichen Bedingung trägt, nämlich "die betroffene Person ist körperlich oder rechtlich nicht in der Lage, ihre Einwilligung zu geben". Diese Formulierung bedeutet, dass der für die Verarbeitung Verantwortliche zuerst versuchen sollte, die Einwilligung der betroffenen Person einzuholen[ix].

3.4. Verarbeitung durch gemeinnützige Körperschaft mit einem politischen, philosophischen, religiösen oder gewerkschaftlichen Ziel

Die Möglichkeit, sensible Daten unter diesem rechtlichen Grund zu verarbeiten, wird bestimmten gemeinnützigen Organisationen wie politischen Parteien, Stiftungen, Kirchen,

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

anderen Formen von philosophischen, religiösen oder gewerkschaftlichen Organisationen gewährt. Solche Organisationen könnten sensible Daten verarbeiten, wenn:

- diese Daten beziehen sich ausschließlich auf die Mitglieder / auf ehemalige Mitglieder der Einrichtung oder auf Personen, die regelmäßig Kontakt mit ihr haben;
- die Verarbeitung erfolgt im Rahmen ihrer legitimen Aktivitäten;
- die Verarbeitung erfolgt in Verbindung mit ihren spezifischen Zwecken;
- es gibt angemessene Garantien für die Rechte der betroffenen Person;
- die personenbezogenen Daten werden ohne die Zustimmung der betroffenen Personen nicht außerhalb dieses Organs weitergegeben.

Weitere spezifische Anforderungen sollten im nationalen Recht angestrebt werden [x].

Dieser rechtliche Grund würde für lokale Behörden im Laufe ihrer Tätigkeit praktisch keine praktische Anwendung finden.

3.5. Die Daten werden offensichtlich von der betroffenen Person veröffentlicht

Werden die personenbezogenen Daten von der betroffenen Person offenkundig an die breite Öffentlichkeit weitergegeben, so wird davon ausgegangen, dass die betroffene Person auf den besonderen Schutz dieser Informationen verzichtet hat. In jedem Fall muss die Entscheidung, solche Informationen offenzulegen, ein Ergebnis der freien Wahl des Einzelnen sein[xi]. Eine solche Offenlegung kann verschiedene Formen annehmen - Daten aus öffentlich zugänglichen Registern, Websites, Listen, Foren oder sogar aus einem Profil in einem sozialen Netzwerk, auf das ohne Benutzerkonto zugegriffen werden kann, usw.[xii] In jedem Fall entbindet die Tatsache, dass solche Daten offenkundig veröffentlicht werden, den für die Verarbeitung Verantwortlichen nicht von der Verpflichtung, die anderen Anforderungen der DSGVO zu erfüllen - z. Einhaltung der Datenschutzgrundsätze, Einhaltung des Datenschutzes durch Datenschutz und Datenschutz durch geeignete Maßnahmen, um die Sicherheit der Daten zu gewährleisten, etc.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

3.6. Begründung, Ausübung oder Verteidigung von Rechtsansprüchen / Gerichten, die in ihrer gerichtlichen Eigenschaft handeln

In bestimmten Fällen kann die Verarbeitung sensibler Daten erforderlich sein, um rechtliche Ansprüche zu begründen, auszuüben oder zu verteidigen. Der für die Verarbeitung Verantwortliche trägt die Beweislast dafür, dass eine solche Verarbeitung erforderlich ist, d.h. Dass eine enge und inhaltliche Verbindung zwischen der Verarbeitung und den Zwecken besteht[xiii]. Solche Situationen können z.B. die Einlegung von Rechtsbehelfen vor den Verwaltungsgerichten, die von den zuständigen Behörden erlassen wurden, wenn die Verarbeitung sensibler Daten im vorangegangenen Verwaltungsverfahren stattgefunden hat; Arbeitskämpfe, bei denen die Gesundheitsdaten der Arbeitnehmer von der lokalen Behörde als Arbeitgeber berücksichtigt werden sollten, usw.

Darüber hinaus könnte die Verarbeitung gerichtlicher Tätigkeiten von Gerichten auch die Verarbeitung solcher Kategorien personenbezogener Daten begründen.

3.7. Erhebliches öffentliches Interesse auf der Grundlage des Rechts der EU oder der Mitgliedstaaten

Diese Bestimmung der Datenschutz-Grundverordnung ermächtigt die Mitgliedstaaten, in ihren nationalen Rechtsvorschriften eine spezifische Hypothese einzuführen, wonach sensible Daten verarbeitet werden könnten, die eine solche Verarbeitung mit erheblichem öffentlichem Interesse rechtfertigen.

Um die Anforderungen der DSGVO zu erfüllen, müssen die Mitgliedstaaten sicherstellen, dass:

die Verarbeitung sollte in einem angemessenen Verhältnis zu dem verfolgten Ziel stehen;

das Wesen des Rechts auf Datenschutz wird respektiert;

die erlassenen Rechtsvorschriften sehen geeignete und spezifische Maßnahmen zum Schutz der Grundrechte und der Interessen der betroffenen Person vor.

Es bleibt abzuwarten, wie diese Chance in Zukunft genutzt wird. Eine fallweise Analyse des jeweiligen lokalen Gesetzes ist für LAs ratsam, um festzustellen, ob sie sich auf einen solchen Grund stützen können.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

3.8. Präventive oder Arbeitsmedizin, Beurteilung der Arbeitsfähigkeit des Arbeitnehmers, medizinische Diagnose, Bereitstellung von Gesundheits- oder Sozialpflege oder Behandlung

Das Verbot der Verarbeitung besonderer Kategorien personenbezogener Daten gilt nicht für die Verarbeitung zu medizinischen / sozialen Zwecken [xiv]. Eine solche Verarbeitung könnte in verschiedenen Bereichen wie Arbeitsmedizin, medizinische Diagnose oder Erbringung von Dienstleistungen im Bereich der sozialen oder medizinischen Versorgung stattfinden. Eine solche Verarbeitung könnte entweder auf der Grundlage des Rechts der EU / der Mitgliedstaaten oder im Rahmen eines Vertrags mit dem Angehörigen der Gesundheitsberufe erfolgen[xv]. Darüber hinaus, Kunst. Art. 9 Abs. 3 DSGVO ermöglicht die Verarbeitung sensibler Daten durch eine zur Verschwiegenheit verpflichtete Person.

Dieser rechtliche Grund gilt für Ärzte, Krankenschwestern und andere Personen, die an der Erbringung von Gesundheitsdienstleistungen beteiligt sind [xvi].

Aus praktischer Sicht würde diese Bestimmung es lokale Behörden in ihrer Eigenschaft als Arbeitgeber ermöglichen, arbeitsmedizinische Dienstleistungen als Teil der größeren Verpflichtung zur Gewährleistung der Arbeitsschutzbedingungen sicherzustellen.

3.9. Öffentliches Interesse im Bereich der öffentlichen Gesundheit

Nach dem 54. Erwägungsgrund der Datenschutz-Grundverordnung sollte "öffentliche Gesundheit" im Einklang mit der Definition der Verordnung (EG) Nr. 1338/2008 ausgelegt werden, dh alle Elemente in Bezug auf Gesundheit, Gesundheitszustand, einschließlich Morbidität und Behinderung, die Determinanten, die Auswirkungen auf Gesundheitszustand, Bedarf an Gesundheitsfürsorge, Ressourcen für die Gesundheitsversorgung, Bereitstellung von und allgemeiner Zugang zu Gesundheitsversorgung sowie Ausgaben und Finanzierung des Gesundheitswesens und die Ursachen der Sterblichkeit.

Gründe, die die Anwendung dieses Rechtsgrundes rechtfertigen könnten, könnten der Schutz vor schwerwiegenden grenzüberschreitenden Gesundheitsbedrohungen oder die Gewährleistung hoher Qualitäts- und Sicherheitsstandards für Gesundheitsversorgung, Medizinprodukte oder Medizinprodukte sein[xvii].

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

Die Verarbeitung von Gesundheitsdaten aus Gründen des öffentlichen Interesses darf nicht dazu führen, dass personenbezogene Daten von Dritten wie Arbeitgebern, Versicherungs- oder Bankunternehmen für andere Zwecke verarbeitet werden.

3.10. Verarbeitung zu Archivierungszwecken im öffentlichen Interesse, zu wissenschaftlichen oder historischen Forschungszwecken oder zu statistischen Zwecken

Die Verarbeitung zu solchen Zwecken sollte auf dem Recht der Mitgliedstaaten / der EU beruhen. Die DSGVO schreibt vor, dass die Rechtsvorschriften, die eine solche Verarbeitung ermöglichen, in einem angemessenen Verhältnis zu dem verfolgten Ziel stehen, den Kern des Rechts auf Datenschutz wahren und geeignete und spezifische Maßnahmen zum Schutz der Grundrechte und der Interessen der betroffenen Person vorsehen. Die eingeführten Garantien müssen der sensiblen Natur der betreffenden personenbezogenen Daten entsprechen[xviii].

3.11. Weitere Bedingungen in den Rechtsvorschriften der Mitgliedstaaten

Artikel 9 Absatz 4 der Datenschutz-Grundverordnung ermächtigt die Mitgliedstaaten, weitere Bedingungen oder Beschränkungen für die Verarbeitung bestimmter besonderer Kategorien personenbezogener Daten einzuführen, und zwar: genetische Daten, biometrische Daten oder Gesundheitsdaten. Daher sollten lokale Gesetze, die für lokale Behörden gelten, in Zukunft überwacht werden.

4. ZUSAMMENFASSUNG & PRAKTISCHE TIPPS

Die lokalen Behörden sollten sich darüber im Klaren sein, dass bestimmte Kategorien personenbezogener Daten einen besonderen Schutz verdienen, da sie inhärent mit den intimsten privaten Bereichen verbunden sind und / oder das Risiko der Diskriminierung

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

beinhalten. Nach allgemeiner Regel ist die Verarbeitung solcher Daten verboten, sofern keine zusätzlichen Bedingungen (Ausnahmen von dieser Regel) vorliegen.

Die praktischsten Aspekte, die sich auf die Tätigkeiten der Gebietskörperschaften auswirken könnten, sind die Verarbeitungstätigkeiten der Gesundheitsdaten der Arbeitnehmer. Die DSGVO gestattet eine solche Verarbeitung, jedoch nur, wenn dies für die Pflicht des Kontrolleurs (oder das Recht der betroffenen Person) nach dem Arbeitsgesetz erforderlich ist.

Die Daten über strafrechtliche Verurteilungen und Straftaten sind keine besondere Kategorie, sondern unterliegen auch einer Sonderregelung im Rahmen der DSGVO. Die Personalpraxis für die Erhebung von Vorstrafen oder umfangreiche Hintergrundkontrollen künftiger Arbeitnehmer sollte im Lichte der Datenschutzgrundverordnung überarbeitet werden.

5. EXTERNE QUELLEN & WEBLINKS

5.1. Bücher

- Boardman, R., Mullock, J., Mole, A. Bird & Bird Guide to General Data Protection Regulation (2016);
- Ehmann, E., Helfrich, M. EG Datenschutzrichtlinie: Kurzkommentar, Verlag Dr. Otto Schmidt, Koln, (1999)
- Voigt, P., von dem Bussche, A., The EU General Data Protection Regulation (GDPR) – A Practical Guide, Springer International Publishing (2017);
- EU General Data Protection Regulation (GDPR). An Implementation and Compliance Guide, IT Governance Publishing, Cambridgeshire (2016);
- European Data Protection. Law and Practice, Executive Editor: Edurado Ustaran, CIPP/E, Partner, Hogan Lovells, IAPP (2018);

5.2. Dokumente der Artikel 29 Working Party

- WP29, Guidelines on Consent under Regulation 2016/679, WP 259;
- WP29, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, WP 217;

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

5.3. Web Links

- http://europa.eu/rapid/press-release_IP-18-386_en.htm
- https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en
- https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/sensitive-data/what-personal-data-considered-sensitive_en
- https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/sensitive-data/under-what-conditions-can-my-company-organisation-process-sensitive-data_en

6. REFERENZEN

[i] Ehmann, E., Helfrich, M. EG Datenschutzrichtlinie: Kurzkommentar, Verlag Dr. Otto Schmidt, Koln, (1999), p. 130-131.
[ii] GDPR explicitly recognizes the term 'sensitive data' – see e.g. Recital 10.
[iii] European Data Protection. Law and Practice, Executive Editor: Edurado Ustaran, CIPP/E, Partner, Hogan Lovells, IAPP (2018), p. 123.
[iv] Ibid, p. 111.
[v] In Bulgaria such data are sensitive since 2005.
[vi] Boardman, R., Mullock, J., Mole, A. Bird & Bird Guide to General Data Protection Regulation (2016), p. 18.
[vii] Voigt, P., von dem Bussche, A., The EU General Data Protection Regulation (GDPR) – A Practical Guide, Springer International Publishing (2017), p. 111.
[viii] EU General Data Protection Regulation (GDPR). An Implementation and Compliance Guide, IT Governance Publishing, Cambridgeshire (2016), p. 196.
[ix] Ibid, p. 126.
[x] Ibid, p. 126-127.
[xi] Voigt, P., von dem Bussche, A., The EU General Data Protection Regulation (GDPR) – A Practical Guide, Springer International Publishing (2017), p. 113.
[xii] Ibid, p. 113.
[xiii] European Data Protection. Law and Practice, Executive Editor: Edurado Ustaran, CIPP/E, Partner, Hogan Lovells, IAPP (2018), p. 127.
[xiv] Ibid, p. 128.
[xv] Ibid, p. 129.
[xvi] Ibid, p. 129.
[xvii] Voigt, P., von dem Bussche, A., The EU General Data Protection Regulation (GDPR) – A Practical Guide, Springer International Publishing (2017), p. 114.
[xviii] Ibid, p. 115.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

ProLegis

ERNENNUNG, POSITION UND AUFGABEN VON DATENSCHUTZ-BEAUFTRAGTEN (DSB)

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

Dissemination Level:		
PU	Public	
CO	Confidential, only for members of the consortium (including the Commission Services)	
EU-RES	Classified Information: RESTREINT UE (Commission Decision 2005/444/EC)	
EU-CON	Classified Information: CONFIDENTIEL UE (Commission Decision 2005/444/EC)	
EU-SEC	Classified Information: SECRET UE (Commission Decision 2005/444/EC)	
Document version control:		
Version	**Author(s)**	**Date**
Version 1	Developed by:	
Version 1	Reviewed & updated by:	
Version 2	Translated by: VICESSE	21/06/18

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

Inhaltsverzeichnis

1. RECHTLICHER RAHMEN 5
1.1. DSGVO 5
2. ERNENNUNG DES DSB 8
2.1. Obligatorische Ernennung nach DSGVO 8
2.1.1. Behörde oder Körperschaft 8
2.1.2. Die Kerntätigkeiten des für die Verarbeitung Verantwortlichen / Prozessors [...] erfordern eine regelmäßige und systematische Überwachung der betroffenen Personen in großem Umfang 9
2.1. Andere Situationen für die Ernennung von DPO 11
2.2.1. Obligatorische Ernennung nach EU / Mitgliedstaat-Recht 11
2.2.2. Freiwillige Ernennung 11
2.3. Vertragsbeziehungen mit dem DSB 12
2.3.1. Arbeitsvertrag 12
2.3.2. Servicevertrag 12
3. POSITION DES DSB 13
3.1. Beteiligung an allen Fragen im Zusammenhang mit dem Schutz personenbezogener Daten 13
3.2. Sicherstellung der notwendigen Ressourcen und Unabhängigkeit 14
3.3. Interessenkonflikt 16
4. AUFGABEN DES DSB 16
4.1. Überwachung 16
4.2. DSFA 17
4.3. Anlaufstelle 17
4.4. Aufzeichnung 18
5. SCHLUSSFOLGERUNG & PRAKTISCHE HINWEISE 18
6. EXTERNE QUELLEN & WEBLINKS 19
6.1. Bücher 19

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

6.2. Dokumente der Artikel 29 Working Party 19
6.3. Web Links 19
7. REFERENZEN 19

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

1. RECHTLICHER RAHMEN

1.1. DSGVO

Artikel 37

Benennung eines Datenschutzbeauftragten

(1) Der Verantwortliche und der Auftragsverarbeiter benennen auf jeden Fall einen Datenschutzbeauftragten, wenn

a) die Verarbeitung von einer Behörde oder öffentlichen Stelle durchgeführt wird, mit Ausnahme von Gerichten, die im Rahmen ihrer justiziellen Tätigkeit handeln,

b) die Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters in der Durchführung von Verarbeitungsvorgängen besteht, welche aufgrund ihrer Art, ihres Um-fangs und/oder ihrer Zwecke eine umfangreiche regelmäßige und systematische Überwachung von betroffenen Personen erforderlich machen, oder

c) die Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters in der umfang-reichen Verarbeitung besonderer Kategorien von Daten gemäß Artikel 9 oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten ge-mäß Artikel 10 besteht.

(2) Eine Unternehmensgruppe darf einen gemeinsamen Datenschutzbeauftragten ernennen, sofern von jeder Niederlassung aus der Datenschutzbeauftragte leicht er-reicht werden kann.

(3) Falls es sich bei dem Verantwortlichen oder dem Auftragsverarbeiter um eine Behörde oder öffentliche Stelle handelt, kann für mehrere solcher Behörden oder Stellen unter Berücksichtigung ihrer Organisationsstruktur und ihrer Größe ein gemeinsamer Datenschutzbeauftragter benannt werden.

(4) In anderen als den in Absatz 1 genannten Fällen können der Verantwortliche o-der der Auftragsverarbeiter oder Verbände und andere Vereinigungen, die Kategorien von Verantwortlichen oder Auftragsverarbeitern vertreten, einen Datenschutzbeauf-tragten benennen; falls dies nach dem Recht der Union oder der Mitgliedstaaten vor-geschrieben ist, müssen sie einen solchen benennen. Der Datenschutzbeauftragte kann für derartige Verbände und andere Vereinigungen, die Verantwortliche oder Auf-tragsverarbeiter vertreten, handeln.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

(5) Der Datenschutzbeauftragte wird auf der Grundlage seiner beruflichen Qualifika-tion und insbesondere des Fachwissens benannt, das er auf dem Gebiet des Daten-schutzrechts und der Datenschutzpraxis besitzt, sowie auf der Grundlage seiner Fä-higkeit zur Erfüllung der in Artikel 39 genannten Aufgaben.

(6) Der Datenschutzbeauftragte kann Beschäftigter des Verantwortlichen oder des Auftragsverarbeiters sein oder seine Aufgaben auf der Grundlage eines Dienstleis-tungsvertrags erfüllen.

(7) Der Verantwortliche oder der Auftragsverarbeiter veröffentlicht die Kontaktdaten des Datenschutzbeauftragten und teilt diese Daten der Aufsichtsbehörde mit.

Artikel 38

Stellung des Datenschutzbeauftragten

(1) Der Verantwortliche und der Auftragsverarbeiter stellen sicher, dass der Daten-schutzbeauftragte ordnungsgemäß und frühzeitig in alle mit dem Schutz personenbe-zogener Daten zusammenhängenden Fragen eingebunden wird.

(2) Der Verantwortliche und der Auftragsverarbeiter unterstützen den Datenschutz-beauftragten bei der Erfüllung seiner Aufgaben gemäß Artikel 39, indem sie die für die Erfüllung dieser Aufgaben erforderlichen Ressourcen und den Zugang zu personen-bezogenen Daten und Verarbeitungsvorgängen sowie die zur Erhaltung seines Fachwissens erforderlichen Ressourcen zur Verfügung stellen.

(3) Der Verantwortliche und der Auftragsverarbeiter stellen sicher, dass der Daten-schutzbeauftragte bei der Erfüllung seiner Aufgaben keine Anweisungen bezüglich der Ausübung dieser Aufgaben erhält. Der Datenschutzbeauftragte darf von dem Ver-antwortlichen oder dem Auftragsverarbeiter wegen der Erfüllung seiner Aufgaben nicht abberufen oder benachteiligt werden. Der Datenschutzbeauftragte berichtet un-mittelbar der höchsten Managementebene des Verantwortlichen oder des Auf-tragsverarbeiters.

(4) Betroffene Personen können den Datenschutzbeauftragten zu allen mit der Verarbeitung ihrer personenbezogenen Daten und mit der Wahrnehmung ihrer Rechte gemäß dieser Verordnung im Zusammenhang stehenden Fragen zu Rate ziehen.

(5) Der Datenschutzbeauftragte ist nach dem Recht der Union oder der Mitgliedstaa-ten bei der Erfüllung seiner Aufgaben an die Wahrung der Geheimhaltung oder der Vertraulichkeit gebunden.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

(6) Der Datenschutzbeauftragte kann andere Aufgaben und Pflichten wahrnehmen. Der Verantwortliche oder der Auftragsverarbeiter stellt sicher, dass derartige Aufgaben und Pflichten nicht zu einem Interessenkonflikt führen.

Artikel 39

Aufgaben des Datenschutzbeauftragten

(1) Dem Datenschutzbeauftragten obliegen zumindest folgende Aufgaben:

a) Unterrichtung und Beratung des Verantwortlichen oder des Auftragsverarbeiters und der Beschäftigten, die Verarbeitungen durchführen, hinsichtlich ihrer Pflichten nach dieser Verordnung sowie nach sonstigen Datenschutzvorschriften der Union bzw. der Mitgliedstaaten;

b) Überwachung der Einhaltung dieser Verordnung, anderer Datenschutzvorschriften der Union bzw. der Mitgliedstaaten sowie der Strategien des Verantwortlichen oder des Auftragsverarbeiters für den Schutz personenbezogener Daten einschließlich der Zuweisung von Zuständigkeiten, der Sensibilisierung und Schulung der an den Verarbeitungsvorgängen beteiligten Mitarbeiter und der diesbezüglichen Überprü-fungen;

c) Beratung — auf Anfrage — im Zusammenhang mit der Datenschutz-Folgenabschätzung und Überwachung ihrer Durchführung gemäß Artikel 35;

d) Zusammenarbeit mit der Aufsichtsbehörde;

e) Tätigkeit als Anlaufstelle für die Aufsichtsbehörde in mit der Verarbeitung zusammenhängenden Fragen, einschließlich der vorherigen Konsultation gemäß Artikel 36, und gegebenenfalls Beratung zu allen sonstigen Fragen.

(2) Der Datenschutzbeauftragte trägt bei der Erfüllung seiner Aufgaben dem mit den Verarbeitungsvorgängen verbundenen Risiko gebührend Rechnung, wobei er die Art, den Umfang, die Umstände und die Zwecke der Verarbeitung berücksichtigt.

Erwägungsgründe

(97) In Fällen, in denen die Verarbeitung durch eine Behörde — mit Ausnahmen von Gerichten oder unabhängigen Justizbehörden, die im Rahmen ihrer justiziellen Tätigkeit handeln –, im privaten Sektor durch einen Verantwortlichen erfolgt, des-sen Kerntätigkeit

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

in Verarbeitungsvorgängen besteht, die eine regelmäßige und systematische Überwachung der betroffenen Personen in großem Umfang erfor-dern, oder wenn die Kerntätigkeit des Verantwortlichen oder des Auftragsverarbei-ters in der umfangreichen Verarbeitung besonderer Kategorien von personenbe-zogenen Daten oder von Daten über strafrechtliche Verurteilungen und Straftaten besteht, sollte der Verantwortliche oder der Auftragsverarbeiter bei der Überwa-chung der internen Einhaltung der Bestimmungen dieser Verordnung von einer weiteren Person, die über Fachwissen auf dem Gebiet des Datenschutzrechts und der Datenschutzverfahren verfügt, unterstützt werden Im privaten Sektor bezieht sich die Kerntätigkeit eines Verantwortlichen auf seine Haupttätigkeiten und nicht auf die Verarbeitung personenbezogener Daten als Nebentätigkeit. Das erforderliche Niveau des Fachwissens sollte sich insbesondere nach den durchgeführten Datenverarbeitungsvorgängen und dem erforderlichen Schutz für die von dem Verantwortlichen oder dem Auftragsverarbeiter verarbeiteten personenbezogenen Daten richten. Derartige Datenschutzbeauftragte sollten unabhängig davon, ob es sich bei ihnen um Beschäftigte des Verantwortlichen handelt oder nicht, ihre Pflichten und Aufgaben in vollständiger Unabhängigkeit ausüben können.

2. ERNENNUNG DES DSB

2.1. Obligatorische Ernennung nach DSGVO

2.1.1. Behörde oder Körperschaft

Die DSGVO enthält keine rechtliche Definition, was unter "Behörde oder Körperschaft" verstanden wird. Ob eine natürliche / juristische Person eine öffentliche Behörde / Stelle darstellt, sollte gemäß den nationalen Rechtsvorschriften des jeweiligen Mitgliedstaats festgelegt werden. Dieses Konzept sollte umfassend ausgelegt werden und umfasst in jedem Fall nationale, regionale und lokale Behörden. Nach WP29 können jedoch auch bestimmte natürliche / juristische Personen einbezogen werden, deren Tätigkeit dem öffentlichen / privaten Recht unterliegt (z. B. öffentliche Verkehrsdienste, Wasser- und Energieversorgung, Straßeninfrastruktur, öffentlich-rechtlicher Rundfunk, Sozialwohnungen oder Disziplinarbehörden für reglementierte Berufe).[i] Die Logik einer solchen Interpretation liegt darin, dass die Bürger (betroffene Personen) nur eine begrenzte Auswahl haben, ob und wie ihre personenbezogenen Daten von solchen Einrichtungen verarbeitet werden. Obwohl eine solche Interpretation nicht zwingend und verbindlich ist, ist eine sorgfältige Abwägung und Analyse innerhalb dieser Organisationen, ob ein DSB zu ernennen ist, empfehlenswert.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

Es sollte angemerkt werden, dass in der WP29 empfohlen wird, einen Datenschutzbeauftragten zu benennen, dessen Funktionen auch alle durchgeführten Verarbeitungsvorgänge umfassen sollten, einschließlich derer, die nicht mit der Erfüllung einer öffentlichen Aufgabe oder der Ausübung einer Amtspflicht zusammenhängen (z. B. die Beziehungen zur Angestellte).[ii] Keine der Bestimmungen der DSGVO erfordert jedoch die Ernennung von DSB lediglich für die Verarbeitungstätigkeit im Zusammenhang mit öffentlichen Aufgaben. Daher ist die angemessenere und sicherste Interpretation, dass lokale Behörden einen DSB ernennt, der für alle Datenverarbeitungsaktivitäten innerhalb der Organisation verantwortlich ist (Beziehungen zu Bürgern, Angestellten, Kandidaten für Arbeit, ehemaligen Angestellten, anderen Behörden usw.).

2.1.2. Die Kerntätigkeiten des für die Verarbeitung Verantwortlichen / Prozessors [...] erfordern eine regelmäßige und systematische Überwachung der betroffenen Personen in großem Umfang

Die Datenverarbeitungsaktivitäten von lokalen Behörden würden generell in den Anwendungsbereich von Punkt 2.1.1 fallen, d. h. lokale Behörden sollten einen DSB auf der Grundlage ihrer Kapazität als öffentlicher Behörde / Stelle ernennen. Aus Gründen der Klarheit wird im Folgenden eine kurze Analyse der beiden anderen Hypothesen im Rahmen der DSGVO vorgenommen, wenn die Bestellung eines DSB obligatorisch sein soll. Diese Informationen können für private Einrichtungen nützlich sein, deren Kapital ganz oder teilweise der Gemeinde oder anderen lokalen Behörden / staatlichen Einrichtungen gehört und die nicht in den Bereich "öffentliche Behörde / Stelle" fallen.

Unter dem Begriff "Kernaktivitäten" sollte man die Schlüsseloperationen verstehen, die notwendig sind, um die Ziele des Controllers oder Prozessors zu erreichen.[iii] Beispiele, die von WP29 gegeben werden, umfassen die Verarbeitung von Gesundheitsakten in Krankenhäusern oder die Überwachung durch private Sicherheitsunternehmen. In der gleichen Zeit sind Standard-IT-Support-Aktivitäten von den "Kernaktivitäten" der Organisation ausgeschlossen.[iv]

Das Konzept "Large Scale" ist in der DSGVO nicht explizit definiert. Es wird ausdrücklich erwähnt, dass eine Verarbeitung auf regionaler, nationaler oder supranationaler Ebene, die eine erhebliche Menge an Daten umfasst und die eine große Anzahl betroffener Personen betreffen könnte und die ein hohes Risiko zur Folge haben könnte, als Verarbeitung im "großen Maßstab" betrachtet werden könnte. Im Gegenteil, Einzelpraktiker wie

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

ein einziger Gesundheitsspezialist oder Jurist verarbeiten keine personenbezogenen Daten im großen Stil.

WP29 enthält eine nicht erschöpfende Liste von Aktivitäten, die als groß angelegte Verarbeitung betrachtet werden könnten:

- Verarbeitung von Patientendaten durch ein Krankenhaus;
- Verarbeitung von Reisedaten von Personen, die das öffentliche Verkehrssystem einer Stadt nutzen (z. B. Tracking über Reisekarten);
- Verarbeitung von Echtzeit-Geopositionsdaten von Kunden einer internationalen Fastfood-Kette für statistische Zwecke durch einen auf die Erbringung dieser Dienstleistungen spezialisierten Verarbeiter;
- Verarbeitung von Kundendaten durch ein Versicherungsunternehmen / eine Bank;
- Verarbeitung personenbezogener Daten für verhaltensbezogene Werbung durch eine Suchmaschine
- Verarbeitung von Daten (Inhalt, Verkehr, Standort) per Telefon oder Internet Service Provider.[v]

Der Begriff "regelmäßig" ist inhärent mit der Verarbeitung verbunden, die entweder permanent (konstant) oder periodisch stattfindet. Der Begriff "systematisches Monitoring" erfordert, dass die Verarbeitung auf einem bestimmten Plan, einer Strategie oder einer ähnlichen vordefinierten Methodik organisiert in einem System stattfindet.[vi] Beispiele umfassen unter anderem das Betreiben von Telekommunikationsnetzwerken, Profiling, Verhaltenswerbung, Verarbeitung von Informationen von intelligenten Geräten usw.

2.1.3 Die Kerntätigkeiten des für die Verarbeitung Verantwortlichen / Auftragsverarbeiters bestehen in der umfangreichen Verarbeitung besonderer Datenkategorien [...] und personenbezogener Daten zu strafrechtlichen Verurteilungen und Straftaten

Für die Begriffe "Kernaktivitäten" und groß angelegte Datensammlungen siehe Punkt 2.1.2. über.

Der Begriff und sollte korrektiv als "oder" interpretiert werden. Mit anderen Worten, jede Verarbeitung, die entweder die Verarbeitung besonderer Datenkategorien oder personenbezogener Daten im Zusammenhang mit strafrechtlichen Verurteilungen und Straftaten umfasst, die in großem Umfang zur Kerntätigkeit der Organisation gehört, sollte die Benennung von DSB erfordern.

Spezielle Datenkategorien sind:

- personenbezogene Daten, aus denen die rassische oder ethnische Herkunft hervorgeht;

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

- politische Meinungen;
- religiöse oder philosophische Überzeugungen;
- Gewerkschaftsmitgliedschaft;
- genetische Daten;
- biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person:
- Daten über Gesundheit oder Daten über das Sexualleben oder die sexuelle Orientierung einer natürlichen Person.

Personenbezogene Daten zu strafrechtlichen Verurteilungen und Straftaten können Informationen enthalten, die in Gerichtsurteilen, Strafregistern oder Akten von Ermittlungsbehörden enthalten sind.

2.1. Andere Situationen für die Ernennung von DPO

2.2.1. Obligatorische Ernennung nach EU / Mitgliedstaat-Recht

Gemäß Artikel 37 Absatz 4 DSGVO können die EU und / oder die Mitgliedstaaten andere Situationen vorsehen, in denen die Ernennung eines DSB obligatorisch ist. Eine solche verbindliche Ernennung kann durch ein qualitatives Zeichen (z. B. für bestimmte sektorspezifische Verarbeitungsaktivitäten) oder durch ein quantitatives Zeichen (z. B. falls die Organisation die persönlichen Daten bestimmter Datensubjekte verarbeitet) erforderlich sein. Deutschland hat beispielsweise in seinen lokalen Datenschutzgesetzen umfassendere Anforderungen als die DSGVO eingeführt: (i) Unternehmen, die in Deutschland tätig sind und mindestens 10 Personen im Bereich der automatisierten Verarbeitung beschäftigen, müssen einen DSB ernennen; (ii) in Fällen der automatisierten Verarbeitung im Geschäftsverkehr zum Zwecke der Übertragung; eine anonymisierte Übertragung; Markt oder Meinung, Unternehmen müssen einen DPO unabhängig von der Anzahl der Beschäftigten für die automatisierte Verarbeitung personenbezogener Daten ernennen[vii].

2.2.2. Freiwillige Ernennung

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

Die DSGVO sieht auch die Möglichkeit vor, freiwillig DSB zu ernennen. Ein solcher Ansatz könnte für Organisationen sinnvoll sein, die die Einhaltung der Datenschutzvorschriften nachweisen und Transparenz und Vertrauen fördern möchten. Da die Tätigkeit der Gebietskörperschaften eher unter die erste zwingende Voraussetzung (Behörde / Einrichtung) fallen würde, könnte die freiwillige Ernennung für bestimmte Organisationen gelten, deren Kapital der Gemeinde / dem Staat gehört - z.B. ÖPNV-Unternehmen, öffentliche Schulen / Universitäten, öffentliche Versorgungsunternehmen (Wasser-, Gas-, Stromversorgung), etc.

2.3. Vertragsbeziehungen mit dem DSB

2.3.1. Arbeitsvertrag

Die DSGVO sieht ausdrücklich die Möglichkeit vor, den Datenschutzbeauftragten auf der Grundlage eines Arbeitsvertrags zu ernennen. Dies impliziert zwei Möglichkeiten: (i) jemanden zu ernennen, der bereits in der Organisation arbeitet, um ihre Funktion mit den Funktionen des Datenschutzbeauftragten zu verbinden, oder (ii) um eine neue Arbeitsposition für den Datenschutzbeauftragten zu schaffen. Die Wahl zwischen diesen beiden Möglichkeiten hängt stark von der Struktur, der Anzahl der Mitarbeiter, der Arbeitsbelastung und der Art und Anzahl der Datenverarbeitungsaktivitäten ab und sollte von Fall zu Fall getroffen werden. Wenn die Organisation der jeweiligen lokalen Behörde eher klein ist, könnte es sinnvoll sein, keinen neuen Mitarbeiter zu ernennen, sondern die Funktion des Datenschutzbeauftragten einer bereits tätigen Person zuzuweisen die Organisation (in jedem Fall sollte ein Interessenkonflikt vermieden werden). Im Gegenteil, wenn die Organisation der lokalen Behörde groß ist und / oder ihre täglichen Aktivitäten mit der Verarbeitung großer Mengen personenbezogener Daten (oder sensibler Daten / Daten im Zusammenhang mit Verurteilungen und Straftaten) zusammenhängen, ist die Wahl einer neuen Position für (zumindest) einen DSB gerechtfertigt.

2.3.2. Servicevertrag

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

Die DSGVO verpflichtet die Organisationen nicht, die Datenschutzbeauftragten nur als Bedienstete zu ernennen. Die Verordnung sieht ausdrücklich vor, dass die Funktion von DSB im Rahmen eines Dienstleistungsvertrags an externe Personen / Organisationen ausgelagert werden kann. In WP29 wird empfohlen, dass externe Teams von behördlichen Datenschutzbeauftragten einen bestimmten leitenden Ansprechpartner und Verantwortlichen für jeden Kunden haben, der im Dienstleistungsvertrag festgelegt werden sollte.[viii] Darüber hinaus sollte jedes Mitglied der externen DSB-Organisation alle anwendbaren Anforderungen im Rahmen der DSGVO erfüllen.

Eine Auslagerung der DPO-Funktionen an eine externe Organisation könnte ebenfalls sinnvoll sein, da eine solche Organisation über das erforderliche Maß an Expertenwissen, Erfahrung und die Beibehaltung relevanter Zertifizierungen verfügen würde.[ix]

Zu guter Letzt könnte der Abschluss eines Dienstleistungsvertrags mit einem externen Datenschutzbeauftragten je nach lokalem Recht die Durchführung bestimmter formeller Verfahren (z. B. nach dem Vergaberecht) erforderlich machen.

3. POSITION DES DSB

3.1. Beteiligung an allen Fragen im Zusammenhang mit dem Schutz personenbezogener Daten

Die DSGVO sieht ausdrücklich vor, dass der Datenschutzbeauftragte in alle Fragen im Zusammenhang mit dem Datenschutz in der Organisation einbezogen werden sollte. WP29 sieht die Beteiligung des Datenschutzbeauftragten (im Hinblick auf Konsultationen, Beratung, Kontrolle usw.) in jedem Prozess, der die Verarbeitung personenbezogener Daten ab dem frühestmöglichen Zeitpunkt umfasst, als eines der Instrumente zur Gewährleistung des Datenschutzes[x].

Zu den praktischen Auswirkungen der Beteiligung von Datenschutzbeauftragten an der Organisation könnten beispielsweise gehören:

- Beratung bei der Durchführung der Datenschutz-Folgenabschätzung (DPIA) (Art. 35 Abs. 2 der DSGVO);
- Teilnahme an Arbeitstreffen (WP29 schreibt die Teilnahme an Sitzungen des oberen und mittleren Managements vor, aber in der Praxis könnte die Interaktion des

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

Datenschutzbeauftragten mit dem Personal auf Expertenebene einen ähnlichen (wenn nicht höheren) Mehrwert haben;
- jedes Mal, wenn eine Verwaltungsentscheidung über die Datenverarbeitung getroffen werden muss, vom Datenschutzbeauftragten Rücksprache zu nehmen;
- Ich möchte vom Datenschutzbeauftragten wissen, welche Maßnahmen zu ergreifen sind, wenn eine Datenverletzung auftritt.

3.2. Sicherstellung der notwendigen Ressourcen und Unabhängigkeit

Der Datenschutzbeauftragte könnte seine Aufgabe nicht ordnungsgemäß erfüllen, wenn er nicht mit den erforderlichen Ressourcen ausgestattet wäre. Die Leitung der Organisation ist daher dafür verantwortlich sicherzustellen, dass der Datenschutzbeauftragte zumindest in Bezug auf Folgendes angemessen geschützt ist:

- **Organisatorische Angelegenheiten:**
  - Der DSB sollte ein Team haben, das sie bei der Ausführung ihrer Aufgaben unterstützt. Dies ist besonders wichtig für größere Organisationen. Selbst die Ernennung mehrerer Datenschutzbeauftragter könnte in bestimmten Fällen die Lösung sein.
  - Zugriff auf alle anderen Teams in der Organisation. Der Datenschutzbeauftragte könnte seine Funktionen nicht ordnungsgemäß ausüben, wenn er nicht ordnungsgemäß mit allen anderen für die Datenverarbeitung zuständigen Teams zusammenarbeitet (z. B. Standesamt und Archivierungsabteilung, Rechtsabteilung, Personalabteilung, Rechnungswesen, IT-Abteilung usw.);
  - Verantwortlich nur vor der höchsten Führung. Die DSGVO sieht ausdrücklich vor, dass der Datenschutzbeauftragte nur für das oberste Management der Organisation verantwortlich sein sollte. Für LAs könnte dies z.B. der Bürgermeister, der Gemeinderat, der Direktor / Vorsitzende der jeweiligen Verwaltungseinheit usw. Diese Anforderung ist sehr wichtig, um die Unabhängigkeit des DSB zu gewährleisten. Wenn die Verbindung des Datenschutzbeauftragten mit dem Management indirekt wäre (z. B. durch Vermittler wie den Leiter der Rechtsabteilung oder der Personalabteilung), könnte der Datenschutzbeauftragte seine Aufgaben nicht ordnungsgemäß wahrnehmen, da sie in einer Situation sein werden, in der der Datenschutzbeauftragte rechenschaftspflichtig ist DPO sollte Kontrolle ausüben.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

- Zeit, um die Funktion auszuführen. Diese Anforderung sollte insbesondere in Fällen beachtet werden, in denen der Datenschutzbeauftragte auf Teilzeitbasis ernannt wird oder der externe Datenschutzbeauftragte zusätzlich zu anderen Aufgaben den Datenschutz wahrnimmt.[xi] WP29 schreibt als eine gute Methode vor, einen Prozentsatz der Zeit für die DPO-Funktion festzulegen, wenn sie nicht auf Vollzeitbasis durchgeführt wird.

- **Finanzangelegenheiten**
  - Der Datenschutzbeauftragte sollte über die notwendigen finanziellen Mittel verfügen, um seine Aufgaben zu erfüllen. Wenn die Organisation kein ausreichendes Budget für Datenschutzaktivitäten bereitstellt, könnte die ordnungsgemäße Ausübung der Funktionen des Datenschutzbeauftragten gefährdet sein.
  - Der Datenschutzbeauftragte sollte über die notwendigen Einrichtungen und Geräte verfügen (Räume, Computer, Internetverbindung, Datenbanken, technische Lösungen wie Softwareprogramme usw.).
- **Bildung ist wichtig** - das Fachwissen des Datenschutzbeauftragten sollte ständig verbessert werden (durch Kurse, Sicherstellung neuer Literatur usw.). Angesichts der Tatsache, dass der Datenschutz ein sehr dynamischer Bereich des menschlichen Wissens ist, ist es verständlich, dass der DSB mit den neuesten Trends und Entwicklungen auf dem neuesten Stand sein sollte, um in Bezug auf den Datenschutz ein möglichst hohes Niveau sicherzustellen die Organisation und die neuesten Herausforderungen im Bereich der technologischen und rechtlichen Entwicklung zu bewältigen.

Ein wichtiger Aspekt der Unabhängigkeit des Datenschutzbeauftragten ist das Verbot, dem Datenschutzbeauftragten für die Erfüllung seiner Aufgaben nachteilige Folgen zuzufügen. Die ungünstigen Folgen können sich auf eine Vielzahl von Situationen beziehen - von Entlassung oder anderen Arten von Disziplinarstrafen bis hin zu Verweigerung von Beförderung, Ablehnung von Leistungen anderer Arbeitnehmer usw. Es könnte erwartet werden, dass die Mitgliedstaaten Änderungen in ihre Arbeitsgesetzgebung aufnehmen und Schutz der behördlichen Datenschutzbeauftragten vor Entlassung für die Zeit während der Ausübung ihrer Funktionen und einige Zeit danach vorsehen.[xii] Gleichzeitig sollte eine angemessene Einfügung dieses Verbots erfolgen - der DSB könnte nicht für die ordnungsgemäße Erbringung seiner Dienste bestraft werden. Wenn der Datenschutzbeauftragte jedoch nicht über die erforderlichen Kenntnisse und Fähigkeiten verfügt, Disziplinarmaßnahmen usw. durchführt, sollten die Organisationen in der Lage sein, sie bei allen in den jeweiligen nationalen Arbeitsgesetzen vorgesehenen Entlassungsgründen zu entlassen.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

3.3. Interessenkonflikt

Wenn der Datenschutzbeauftragte im Rahmen eines Arbeitsvertrags benannt wird, darf diese Benennung nicht zu einem Interessenkonflikt führen. Ein Interessenkonflikt könnte entstehen, wenn der DSB eine andere Funktion innerhalb der Organisation hat, die die Zwecke und die Mittel zur Datenverarbeitung innerhalb eines gegebenen internen Prozesses bestimmt. Mit anderen Worten, der DSB könnte nicht gleichzeitig Direktor, Geschäftsführer, Chief Operating, Chief Financial Officer, Chief Medical Officer, Leiter der Marketingabteilung, Leiter der Personalabteilung oder Leiter der IT-Abteilungen sein.[xiii] Darüber hinaus können andere Rollen in der Organisationsstruktur zu Interessenkonflikten führen, wenn solche Positionen oder Rollen zur Bestimmung von Zwecken und Mitteln der Verarbeitung führen (z. B. Buchhalter, Rechtsberater, IT-Spezialist).

Ein Interessenkonflikt kann nicht nur bei der Benennung von DSB im Rahmen eines Arbeitsvertrags entstehen, sondern auch bei einem externen DSB. Wenn der Datenschutzbeauftragte gebeten wird, den für die Verarbeitung Verantwortlichen in Fragen des Datenschutzes vor Gericht zu vertreten, würde ein Interessenkonflikt entstehen, da der Verantwortliche und der Auftragsverarbeiter widersprechende Interessen haben.

4. AUFGABEN DES DSB

4.1. Überwachung

Eine der Hauptaufgaben des Datenschutzbeauftragten besteht darin, alle Datenverarbeitungsaktivitäten innerhalb der Organisation zu überwachen. Dies ist inhärent mit dem Empfang / Sammeln von Informationen, der internen Analyse dieser Informationen und dem Vornehmen von Klarstellungen, Empfehlungen und Empfehlungen innerhalb der Organisation verbunden. Die Überwachungsfunktion konzentriert sich auf die internen Prozesse innerhalb der Organisation. Daher sollte nicht nur das Management informiert und beraten werden, sondern auch die regulären Mitarbeiter auf Expertenebene, deren Aufgaben mit der Verarbeitung personenbezogener Daten verbunden sind.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

4.2. DSFA

Die DSGVO sieht vor, dass der Datenschutzbeauftragte mit beratenden Funktionen in die Datenschutzbehörde einbezogen werden sollte. WP29 empfiehlt als eine gute Vorgehensweise, sich bei einem oder mehreren der folgenden Probleme im Zusammenhang mit der Folgenabschätzung vom Datenschutzbeauftragten beraten zu lassen:

- ob überhaupt eine DSFA durchgeführt werden soll;
- Welche Methodik sollte bei der Durchführung einer DPIA beachtet werden?
- ob die DSFA intern durchgeführt oder ausgelagert werden soll;
- welche Maßnahmen (einschließlich technischer und organisatorischer Maßnahmen) ergriffen werden müssen, um etwaige Risiken für die Rechte und Interessen der betroffenen Personen zu mindern;
- ob die Folgenabschätzung für den Datenschutz korrekt durchgeführt wurde und ob ihre Schlussfolgerungen der DSGVO entsprechen[xiv].

Entscheidet sich das Management der Organisation, im Rahmen des Rechenschaftspflichtgrundsatzes von den Empfehlungen des Datenschutzbeauftragten abzuweichen, empfiehlt es sich, diese Entscheidung und die Gründe dafür zu dokumentieren und diese im Falle einer Prüfung den Aufsichtsbehörden vorlegen zu können.

4.3. Anlaufstelle

Der Datenschutzbeauftragte ist die Hauptansprechstelle sowohl für die Aufsichtsbehörden (Art. 39, Abs. 1, "e" der Datenschutz-Grundverordnung) als auch für die betroffenen Personen (Art. 38 Abs. 4 der Datenschutz-Grundverordnung) in allen Fragen des Datenschutzes die Organisation. Daher ist es von größter Wichtigkeit, die Kontaktdaten des Datenschutzbeauftragten der Aufsichtsbehörde und den betroffenen Personen ordnungsgemäß zu übermitteln. Darüber hinaus ist das Erfordernis, die Kontaktdaten des Datenschutzbeauftragten bereitzustellen, eines der Elemente des Transparenzgrundsatzes nach Art. 12, 13 und 14 der DSGVO.

Nichts in der DSGVO verhindert, dass der Datenschutzbeauftragte die Möglichkeit hat, die Aufsichtsbehörden zu Fragen des Datenschutzes in der Organisation zu konsultieren.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

4.4. Aufzeichnung

Obwohl die Pflicht, Aufzeichnungen über die Verarbeitungstätigkeiten zu führen, nur für die für die Verarbeitung Verantwortlichen und die Verarbeitungsunternehmen und nicht für die Datenschutzbeauftragten gilt, schließt die DSGVO Organisationen nicht aus, diese Funktion dem Datenschutzbeauftragten zuzuweisen. Die Aufgaben des Datenschutzbeauftragten, die in der Datenschutz-Grundverordnung aufgeführt sind, sind nur ein Mindestmaß, daher steht es Organisationen frei, nach eigenem Ermessen andere Aufgaben an den Datenschutzbeauftragten zu delegieren. WP29 betrachtet die Zuweisung der Verpflichtung zur Aufzeichnungspflicht an den Datenschutzbeauftragten als eines der Instrumente, die es dem Datenschutzbeauftragten ermöglichen, seine Aufgaben der Überwachung der Einhaltung zu erfüllen und den Kontrolleur / den Auftragsverarbeiter zu informieren und zu informieren. [xv] Da die Aufzeichnungen ein wirksames Instrument zur Gewährleistung der Rechenschaftspflicht darstellen, könnte es sinnvoll sein, diese Verpflichtung dem DSB zu übertragen.

5. SCHLUSSFOLGERUNG & PRAKTISCHE HINWEISE

Der Datenschutzbeauftragte ist eine der Schlüsselfiguren für die Einhaltung der neuen Datenschutzvorschriften. Die Bedeutung dieser Rolle hängt weitgehend von der jeweiligen Organisation selbst ab. Wenn die Organisation den Datenschutzbeauftragten in allen Fragen des Datenschutzes ordnungsgemäß einbindet und die erforderlichen Ressourcen für die Wahrnehmung ihrer Aufgaben durch den Datenschutzbeauftragten sicherstellt, könnte Datenschutzbeauftragter einer der entscheidenden Faktoren sein, um die Einhaltung sicherzustellen und das Vertrauen in der Gesellschaft zu stärken. Wäre dies nicht der Fall, wäre der DSB eine eher illusorische Figur ohne wirkliche Funktionen als die Verwaltung der Kommunikation im Zusammenhang mit dem Datenschutz, was nicht die Idee dieser Rolle im Rahmen der DSGVO ist.

Die lokale Behörden sollten ermutigt werden, qualifizierte Datenschutzbeauftragte zu benennen, was angesichts des Mangels an auf EU-Ebene vorbereiteten Personen zu einer schwierigen Aufgabe werden könnte. In jedem Fall werden die nächsten Jahre vorgeben, wie sich die Rolle der Datenschutzbeauftragten entwickeln wird. In jedem Fall wäre es

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

positiv für die Gesellschaft, wenn die Las eines der wegweisenden Beispiele dafür wären, wie man die Figur der DSB am besten nutzen könnte.

6. EXTERNE QUELLEN & WEBLINKS

6.1. Bücher

- Harting, N. Datenschutz-Grundverordnung: Das neue Datenschutzrecht in der betrieblichen Praxis, Verlag Dr. Otto Schmidt KG, Köln, 2016;
- Voigt, P., von dem Bussche, A. The EU General Data Protection Regulation (GDPR) – A Practical Guide, Springer International Publishing (2017);
- Boardman, R., Mullock, J., Mole, A. Bird & Bird Guide to General Data Protection Regulation (2016);
- EU General Data Protection Regulation (GDPR). An Implementation and Compliance Guide, IT Governance Publishing, Cambridgeshire (2016);

6.2. Dokumente der Artikel 29 Working Party

- WP29, Guidelines on Data Protection Officers ('DPOs'), WP 243 rev.01;

6.3. Web Links

- http://europa.eu/rapid/press-release_IP-18-386_en.htm
- https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en

7. REFERENZEN

[i] WP29, Guidelines on Data Protection Officers ('DPOs'), WP 243 rev.01, p. 6.
[ii] Ibid.
[iii] Ibid.
[iv] Ibid, p. 6-7.
[v] Ibid, p. 8.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

[vi] Siehe Interpretation der WP29 in WP29, Guidelines on Data Protection Officers ('DPOs'), WP 243 rev.01, p. 8.
[vii] Demmel, A. The Nes German Federal Data Protection Act, Squire Patton Boggs, URL: <https://www.squirepattonboggs.com/~/media/files/insights/publications/2017/09/the-new-german-federal-data-protection-act/27836--german-federal-data-protection-alert.pdf> (26.03.2018);
[viii] WP29, Guidelines on Data Protection Officers ('DPOs'), WP 243 rev.01, p. 22-23.
[ix] EU General Data Protection Regulation (GDPR). An Implementation and Compliance Guide, IT Governance Publishing, Cambridgeshire (2016), p. 58.
[x] WP29, Guidelines on Data Protection Officers ('DPOs'), WP 243 rev.01, p. 13.
[xi] Ibid, p. 14.
[xii] Siehe Demmel, A. The New German Federal Data Protection Act, Squire Patton Boggs, URL: <https://www.squirepattonboggs.com/~/media/files/insights/publications/2017/09/the-new-german-federal-data-protection-act/27836--german-federal-data-protection-alert.pdf> (26.03.2018);
[xiii] WP29, Guidelines on Data Protection Officers ('DPOs'), WP 243 rev.01, p. 16.
[xiv] Ibid, p.17.
[xv] WP29, Guidelines on Data Protection Officers ('DPOs'), WP 243 rev.01, p. 19.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

ProLegis

DATENSCHUTZ-FOLGENABSCHÄTZUNG

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

Dissemination Level:		
PU	Public	
CO	Confidential, only for members of the consortium (including the Commission Services)	
EU-RES	Classified Information: RESTREINT UE (Commission Decision 2005/444/EC)	
EU-CON	Classified Information: CONFIDENTIEL UE (Commission Decision 2005/444/EC)	
EU-SEC	Classified Information: SECRET UE (Commission Decision 2005/444/EC)	

Document version control:		
Version	**Author(s)**	**Date**
Version 1	Developed by:	
Version 1	Reviewed & updated by:	
Version 2	Translated by: VICESSE	21/06/18

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

Inhaltsverzeichnis

1. RECHTLICHER RAHMEN 5
1.1. DSGVO 5
2. IN WELCHEN FÄLLEN IST EINE DSFA ERFORDERLICH? 10
2.1. Grundlagen 10
2.2. Zwingende Fälle für eine DSFA 11
2.2.1. Weitere Prüfung zur Notwendigkeit einer DSFA 12
2.2.2. DSFA für mehrere ähnliche Verarbeitungsvorgänge 13
2.2.3. Positiv- und Negativlisten zur DSFA 13
2.3. Zeitpunkt der Durchführung einer DSFA 14
2.4. Überprüfung der DSFA 15
2.5. Konsultation der Aufsichtsbehörde gemäß Art 36 DSGVO 16
3. WER HAT EINE DATENSCHUTZ-FOLGENABSCHÄTZUNG DURCHZUFÜHREN? 16
3.1. Grundlagen 16
3.2. Mitarbeit an der DSFA – wer soll einbezogen werden 17
4. WIE IST EINE DATENSCHUTZ-FOLGENABSCHÄTZUNG DURCHZUFÜHREN? 18
4.1. Grundlagen 18
4.2. Aufbau einer DSFA 18
4.3. Mindestinhalt einer DSFA 19
4.4. Der Prozess einer Datenschutz-Folgenabschätzung 20
4.5. Die Einbindung betroffener Personen oder ihrer Vertreter 22
4.6. Der Bericht über die Durchführung einer Datenschutz-Folgenabschätzung 23
5. SCHLUSSFOLGERUNGEN UND PRAXISTIPS 26
6. EXTERNE QUELLEN & WEBLINKS 27
6.1. Bücher 27
6.2. Dokumente der Artikel 29 Working Party 27

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

6.3. Web Links 27

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

1. RECHTLICHER RAHMEN

1.1. DSGVO

Artikel 35

Datenschutz-Folgenabschätzung

(1) Hat eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge, so führt der Verantwortliche vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durch. Für die Untersuchung mehrerer ähnlicher Verarbeitungsvorgänge mit ähnlich hohen Risiken kann eine einzige Abschätzung vorgenommen werden.

(2) Der Verantwortliche holt bei der Durchführung einer Datenschutz-Folgenabschätzung den Rat des Datenschutzbeauftragten, sofern ein solcher benannt wurde, ein.

(3) Eine Datenschutz-Folgenabschätzung gemäß Absatz 1 ist insbesondere in folgenden Fällen erforderlich:

a) systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen, die sich auf automatisierte Verarbeitung einschließlich Profiling gründet und die ihrerseits als Grundlage für Entscheidungen dient, die Rechtswirkung gegenüber natürlichen Personen entfalten oder diese in ähnlich erheblicher Weise beeinträchtigen;

b) umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten gemäß Artikel 9 Absatz 1 oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Artikel 10 oder

c) systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche.

(4) Die Aufsichtsbehörde erstellt eine Liste der Verarbeitungsvorgänge, für die gemäß Absatz 1 eine Datenschutz- Folgenabschätzung durchzuführen ist, und veröffentlicht diese. Die Aufsichtsbehörde übermittelt diese Listen dem in Artikel 68 genannten Ausschuss.

(5) Die Aufsichtsbehörde kann des Weiteren eine Liste der Arten von Verarbeitungsvorgängen erstellen und veröffentlichen, für die keine Datenschutz-

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

Folgenabschätzung erforderlich ist. Die Aufsichtsbehörde übermittelt diese Listen dem Ausschuss.

(6) Vor Festlegung der in den Absätzen 4 und 5 genannten Listen wendet die zuständige Aufsichtsbehörde das Kohärenzverfahren gemäß Artikel 63 an, wenn solche Listen Verarbeitungstätigkeiten umfassen, die mit dem Angebot von Waren oder Dienstleistungen für betroffene Personen oder der Beobachtung des Verhaltens dieser Personen in mehreren Mitgliedstaaten im Zusammenhang stehen oder die den freien Verkehr personenbezogener Daten innerhalb der Union erheblich beeinträchtigen könnten.

(7) Die Folgenabschätzung enthält zumindest Folgendes:

a) eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung, gegebenenfalls einschließlich der von dem Verantwortlichen verfolgten berechtigten Interessen;

b) eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck;

c) eine Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen gemäß Absatz 1 und

d) die zur Bewältigung der Risiken geplanten Abhilfemaßnahmen, einschließlich Garantien, Sicherheitsvorkehrungen und Verfahren, durch die der Schutz personenbezogener Daten sichergestellt und der Nachweis dafür erbracht wird, dass diese Verordnung eingehalten wird, wobei den Rechten und berechtigten Interessen der betroffenen Personen und sonstiger Betroffener Rechnung getragen wird.

(8) Die Einhaltung genehmigter Verhaltensregeln gemäß Artikel 40 durch die zuständigen Verantwortlichen oder die zuständigen Auftragsverarbeiter ist bei der Beurteilung der Auswirkungen der von diesen durchgeführten Verarbeitungsvorgänge, insbesondere für die Zwecke einer Datenschutz-Folgenabschätzung, gebührend zu berücksichtigen.

(9) Der Verantwortliche holt gegebenenfalls den Standpunkt der betroffenen Personen oder ihrer Vertreter zu der beabsichtigten Verarbeitung unbeschadet des Schutzes gewerblicher oder öffentlicher Interessen oder der Sicherheit der Verarbeitungsvorgänge ein.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

(10) Falls die Verarbeitung gemäß Artikel 6 Absatz 1 Buchstabe c oder e auf einer Rechtsgrundlage im Unionsrecht oder im Recht des Mitgliedstaats, dem der Verantwortliche unterliegt, beruht und falls diese Rechtsvorschriften den konkreten Verarbeitungsvorgang oder die konkreten Verarbeitungsvorgänge regeln und bereits im Rahmen der allgemeinen Folgenabschätzung im Zusammenhang mit dem Erlass dieser Rechtsgrundlage eine Datenschutz-Folgenabschätzung erfolgte, gelten die Absätze 1 bis 7 nur, wenn es nach dem Ermessen der Mitgliedstaaten erforderlich ist, vor den betreffenden Verarbeitungstätigkeiten eine solche Folgenabschätzung durchzuführen.

(11) Erforderlichenfalls führt der Verantwortliche eine Überprüfung durch, um zu bewerten, ob die Verarbeitung gemäß der Datenschutz-Folgenabschätzung durchgeführt wird; dies gilt zumindest, wenn hinsichtlich des mit den Verarbeitungsvorgängen verbundenen Risikos Änderungen eingetreten sind.

Erwägungsgründe

(89) Gemäß der Richtlinie 95/46/EG waren Verarbeitungen personenbezogener Daten bei den Aufsichtsbehörden generell meldepflichtig. Diese Meldepflicht ist mit einem bürokratischen und finanziellen Aufwand verbunden und hat dennoch nicht in allen Fällen zu einem besseren Schutz personenbezogener Daten geführt. Diese unterschiedslosen allgemeinen Meldepflichten sollten daher abgeschafft und durch wirksame Verfahren und Mechanismen ersetzt werden, die sich stattdessen vorrangig mit denjenigen Arten von Verarbeitungsvorgängen befassen, die aufgrund ihrer Art, ihres Umfangs, ihrer Umstände und ihrer Zwecke wahrscheinlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen mit sich bringen. Zu solchen Arten von Verarbeitungsvorgängen gehören insbesondere solche, bei denen neue Technologien eingesetzt werden oder die neuartig sind und bei denen der Verantwortliche noch keine Datenschutz-Folgenabschätzung durchgeführt hat bzw. bei denen aufgrund der seit der ursprünglichen Verarbeitung vergangenen Zeit eine Datenschutz-Folgenabschätzung notwendig geworden ist.

(90) In derartigen Fällen sollte der Verantwortliche vor der Verarbeitung eine Datenschutz-Folgenabschätzung durchführen, mit der die spezifische Eintrittswahrscheinlichkeit und die Schwere dieses hohen Risikos unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung und der Ursachen des Risikos bewertet werden. Diese Folgenabschätzung sollte sich insbesondere mit den Maßnahmen, Garantien und Verfahren befassen, durch die dieses Risiko eingedämmt,

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

der Schutz personenbezogener Daten sichergestellt und die Einhaltung der Bestimmungen dieser Verordnung nachgewiesen werden soll.

(91) Dies sollte insbesondere für umfangreiche Verarbeitungsvorgänge gelten, die dazu dienen, große Mengen personenbezogener Daten auf regionaler, nationaler oder supranationaler Ebene zu verarbeiten, eine große Zahl von Personen betreffen könnten und — beispielsweise aufgrund ihrer Sensibilität — wahrscheinlich ein hohes Risiko mit sich bringen und bei denen entsprechend dem jeweils aktuellen Stand der Technik in großem Umfang eine neue Technologie eingesetzt wird, sowie für andere Verarbeitungsvorgänge, die ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen mit sich bringen, insbesondere dann, wenn diese Verarbeitungsvorgänge den betroffenen Personen die Ausübung ihrer Rechte erschweren. Eine Datenschutz-Folgenabschätzung sollte auch durchgeführt werden, wenn die personenbezogenen Daten für das Treffen von Entscheidungen in Bezug auf bestimmte natürliche Personen im Anschluss an eine systematische und eingehende Bewertung persönlicher Aspekte natürlicher Personen auf der Grundlage eines Profilings dieser Daten oder im Anschluss an die Verarbeitung besonderer Kategorien von personenbezogenen Daten, biometrischen Daten oder von Daten über strafrechtliche Verurteilungen und Straftaten sowie damit zusammenhängende Sicherungsmaßregeln verarbeitet werden. Gleichermaßen erforderlich ist eine Datenschutz-Folgenabschätzung für die weiträumige Überwachung öffentlich zugänglicher Bereiche, insbesondere mittels optoelektronischer Vorrichtungen, oder für alle anderen Vorgänge, bei denen nach Auffassung der zuständigen Aufsichtsbehörde die Verarbeitung wahrscheinlich ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen mit sich bringt, insbesondere weil sie die betroffenen Personen an der Ausübung eines Rechts oder der Nutzung einer Dienstleistung bzw. Durchführung eines Vertrags hindern oder weil sie systematisch in großem Umfang erfolgen. Die Verarbeitung personenbezogener Daten sollte nicht als umfangreich gelten, wenn die Verarbeitung personenbezogene Daten von Patienten oder von Mandanten betrifft und durch einen einzelnen Arzt, sonstigen Angehörigen eines Gesundheitsberufes oder Rechtsanwalt erfolgt. In diesen Fällen sollte eine Datenschutz-Folgenabschätzung nicht zwingend vorgeschrieben sein.

(92) Unter bestimmten Umständen kann es vernünftig und unter ökonomischen Gesichtspunkten zweckmäßig sein, eine Datenschutz-Folgenabschätzung nicht lediglich auf ein bestimmtes Projekt zu beziehen, sondern sie thematisch breiter anzulegen — beispielsweise wenn Behörden oder öffentliche Stellen eine gemeinsame Anwendung oder Verarbeitungsplattform schaffen möchten oder wenn mehrere Verantwortliche eine gemeinsame Anwendung oder Verarbeitungsumgebung für einen gesamten

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

Wirtschaftssektor, für ein bestimmtes Marktsegment oder für eine weit verbreitete horizontale Tätigkeit einführen möchten.

(93) Anlässlich des Erlasses des Gesetzes des Mitgliedstaats, auf dessen Grundlage die Behörde oder öffentliche Stelle ihre Aufgaben wahrnimmt und das den fraglichen Verarbeitungsvorgang oder die fraglichen Arten von Verarbeitungsvorgängen regelt, können die Mitgliedstaaten es für erforderlich erachten, solche Folgeabschätzungen vor den Verarbeitungsvorgängen durchzuführen.

(94) Geht aus einer Datenschutz-Folgenabschätzung hervor, dass die Verarbeitung bei Fehlen von Garantien, Sicherheitsvorkehrungen und Mechanismen zur Minderung des Risikos ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen mit sich bringen würde, und ist der Verantwortliche der Auffassung, dass das Risiko nicht durch in Bezug auf verfügbare Technologien und Implementierungskosten vertretbare Mittel eingedämmt werden kann, so sollte die Aufsichtsbehörde vor Beginn der Verarbeitungstätigkeiten konsultiert werden. Ein solches hohes Risiko ist wahrscheinlich mit bestimmten Arten der Verarbeitung und dem Umfang und der Häufigkeit der Verarbeitung verbunden, die für natürliche Personen auch eine Schädigung oder eine Beeinträchtigung der persönlichen Rechte und Freiheiten mit sich bringen können. Die Aufsichtsbehörde sollte das Beratungsersuchen innerhalb einer bestimmten Frist beantworten. Allerdings kann sie, auch wenn sie nicht innerhalb dieser Frist reagiert hat, entsprechend ihren in dieser Verordnung festgelegten Aufgaben und Befugnissen eingreifen, was die Befugnis einschließt, Verarbeitungsvorgänge zu untersagen. Im Rahmen dieses Konsultationsprozesses kann das Ergebnis einer im Hinblick auf die betreffende Verarbeitung personenbezogener Daten durchgeführten Datenschutz-Folgenabschätzung der Aufsichtsbehörde unterbreitet werden; dies gilt insbesondere für die zur Eindämmung des Risikos für die Rechte und Freiheiten natürlicher Personen geplanten Maßnahmen.

(95) Der Auftragsverarbeiter sollte erforderlichenfalls den Verantwortlichen auf Anfrage bei der Gewährleistung der Einhaltung der sich aus der Durchführung der Datenschutz-Folgenabschätzung und der vorherigen Konsultation der Aufsichtsbehörde ergebenden Auflagen unterstützen.

(96) Eine Konsultation der Aufsichtsbehörde sollte auch während der Ausarbeitung von Gesetzes- oder Regelungsvorschriften, in denen eine Verarbeitung personenbezogener Daten vorgesehen ist, erfolgen, um die Vereinbarkeit der geplanten Verarbeitung mit dieser Verordnung sicherzustellen und insbesondere das mit ihr für die betroffene Person verbundene Risiko einzudämmen.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

Art 35 DSGVO steht in engem Zusammenhang mit den Art 24, 25 und 32. Ein wesentlicher Unterschied in der Stoßrichtung von Art 32 gegenüber jener von Art 35 besteht darin, dass Art 32 (Sicherheit der Verarbeitung) vor allem auf Risiken abzielt, die von unerwünschten Ereignissen, wie insbesondere Angriffen, ausgehen, während die **Datenschutz-Folgenabschätzung nach Art 35 insbesondere auch jene Risiken betrachtet, die bei regulärem Betrieb von der geplanten Datenverarbeitung an sich ausgehen** bzw ausgehen würden.

Die DSFA ist ein wesentliches Instrument zur Umsetzung des in Art 25 Abs 1 vorgesehenen Datenschutzes durch Technikgestaltung (Privacy by Design). Beiden Konzepten liegt das Prinzip zugrunde, Risiken rechtzeitig vor der Gestaltung der Verarbeitungssysteme zu identifizieren, um in der Gestaltung der Systeme entsprechende Gegenmaßnahmen zu berücksichtigen.

Die DSFA ist das Instrument, um diese Risiken zu erkennen und zu analysieren. Besteht keine Pflicht zur Durchführung einer DSFA, ist dennoch eine Analyse der Datenschutzrisiken erforderlich, um Art 25 und 32 angemessen umsetzen zu können. Beide Bestimmungen sprechen die Risiken für die Rechte und Freiheiten natürlicher Personen ausdrücklich an. Wie umfangreich und formalistisch diese Risikoanalyse ausfällt, hängt von der Komplexität und grundsätzlichen Risikogeneigtheit der Verarbeitung ab. In jedem Fall ist anzuraten, die Risikoanalyse schriftlich zu dokumentieren.

Die Umsetzung des Prinzips Privacy by Design geht jedoch über jene Risiken hinaus, die im Vorfeld durch eine Risikoanalyse explizit erkannt werden können, und umfasst auch Ad-hoc-Entscheidungen der Entwickler (Privacy Engineering), zB zur Umsetzung des Prinzips der Datenminimierung.

2. IN WELCHEN FÄLLEN IST EINE DSFA ERFORDERLICH?

2.1. Grundlagen

Die DSFA ist vorab durchzuführen, dh vor der Aufnahme der Verarbeitung personenbezogener Daten, die ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge haben könnte.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

Grundsätzlich ist für jede Datenverarbeitung eine DSFA durchzuführen, sofern nicht a priori ausgeschlossen werden kann, dass sie voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat. Wann nun ein solches hohes Risiko gegeben ist, lässt sich etwa den Faktoren in Art 35 Abs 3 bzw Erwägungsgrund 91 entnehmen. Hervorgehoben wird insbesondere die Verwendung neuer Technologien, ein unbestimmter Begriff, der in der DSGVO nur im Zusammenhang mit der DSFA verwendet wird. Erforderlich ist lediglich, dass ein hohes Risiko voraussichtlich eintritt, nicht, dass ein solches feststeht; es ist daher eine Prognose zu treffen und die Einschätzung zu dokumentieren.

Art 35 Abs 1 letzter Satz iVm ErwGr 92 bietet einen für die Praxis wichtigen Betrachtungswinkel, für die Beurteilung der Notwendigkeit einer Folgenabschätzung: „Unter bestimmten Umständen kann es vernünftig und unter ökonomischen Gesichtspunkten zweckmäßig sein, eine Datenschutz-Folgenabschätzung nicht lediglich auf ein bestimmtes Projekt zu beziehen, sondern sie thematisch breiter anzulegen — beispielsweise wenn Behörden oder öffentliche Stellen eine gemeinsame Anwendung oder Verarbeitungsplattform schaffen möchten oder wenn mehrere Verantwortliche eine gemeinsame Anwendung oder Verarbeitungsumgebung für einen gesamten Wirtschaftssektor, für ein bestimmtes Marktsegment oder für eine weit verbreitete horizontale Tätigkeit einführen möchten."

2.2. Zwingende Fälle für eine DSFA

Art 35 Abs 3 nennt Fälle, in denen zwingend eine DSFA durchzuführen ist:

a) systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen, die sich auf automatisierte Verarbeitung einschließlich Profiling gründet und die ihrerseits als Grundlage für Entscheidungen dient, die Rechtswirkung gegenüber natürlichen Personen entfalten oder diese in ähnlich erheblicher Weise beeinträchtigen;

b) umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten gemäß Artikel 9 Absatz 1 oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Artikel 10 oder

c) systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

2.2.1. Weitere Prüfung zur Notwendigkeit einer DSFA

Darüber hinaus ist ErwGr 91 zu entnehmen, welche weiteren Fälle eine DSFA erforderlich machen:

a) Verarbeitungsvorgänge, die potenziell eine große Zahl von Personen betreffen, ein hohes Risiko mit sich bringen und bei denen entsprechend dem jeweils aktuellen Stand der Technik in großem Umfang eine neue Technologie eingesetzt wird
b) Verarbeitungsvorgänge ein hohes Risiko mit sich bringen, und betroffenen Personen die Ausübung der Rechte erschweren
c) Verarbeitungsvorgänge, bei denen personenbezogenen Daten für das Treffen von Entscheidungen in Bezug auf bestimmte natürliche Personen im Anschluss an die Verarbeitung besondere Kategorien von personenbezogenen Daten, biometrischen Daten oder von Daten über strafrechtliche Verurteilungen und Straftaten sowie damit zusammenhängende Sicherungsmaßregeln erarbeitet werden
d) Verarbeitungsvorgänge, die ein hohes Risiko mit sich bringen, weil sie die betroffenen Personen an der Ausübung eines Rechts oder der Nutzung einer Dienstleistung bzw. Durchführung eines Vertrages hindern
e) Verarbeitungsvorgänge, die ein hohes Risiko mit sich bringen, weil sie systematisch in großem Umfang erfolgen

Ein Weiterer Prüfschritt zur Frage, ob eine Datenschutz-Folgenabschätzung vorzunehmen ist, werden in Zukunft die Positiv- bzw Negativlisten der Aufsichtsbehörden sein.[1] Diese Listen definieren Verarbeitungsvorgänge, die jedenfalls einer DSFA bedürfen („Positivliste“), bzw solche, bei denen eine DSFA unterbleiben kann („Negativliste“). Beide Listen sind von den Aufsichtsbehörden der Mitgliedstaaten dem Europäischen Datenschutzausschuss im Rahmen des aufsichtsbehördlichen Kohärenzverfahrens zu übermitteln (Art 35 Abs 4), dies mit dem Ziel der Harmonisierung.

Die Artikel-29-Datenschutzgruppe empfielt in Fällen, in denen die Notwendigkeit einer Folgenabschätzung unklar ist, dennoch eine Durchführung, sei es auch nur als Hilfsmittel,

1 Vgl Art 35 Abs 4 und 5.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

um die datenschutzrechtlichen Vorgaben zu erfüllen.[2] Bemerkenswert ist dabei auch, dass die Artikel 29-Datenschutzgruppe in der finalen Empfehlen vom Oktover 2017[3] deutlich zum Ausdruck bringt, dass auch für Anwendungen, die seit dem 25.5.2016 – also ab der Kundmachung und der Vorbereitungszeit auf die allgemeine Wirksamkeit der DSGVO – bereits bestehen, eine Datenschutz-Folgenabschätzung durchzuführen ist. Das hängt damit zusammen, dass die DSGVO bereits seit zwei Jahren in Kraft ist aber erst seit 25.5.2018 allgemein verbindlich und durchsetzbar.

2.2.2. DSFA für mehrere ähnliche Verarbeitungsvorgänge

Der Verantwortliche hat gemäß Art 35 Abs 1 die Möglichkeit, für mehrere ähnliche Verarbeitungsvorgänge mit ähnlich hohem Risiko eine einzige Folgenabschätzung vorzunehmen. Die Beurteilung der Ähnlichkeit bezieht sich diesbezüglich auf die Verarbeitungszwecke. Erwägungsgrund 92 ist dazu zu entnehmen, dass unter Berücksichtigung von ökonomischen Gesichtspunkten eine DSFA thematisch breiter angelegt werden kann, etwa wenn mehrere Verantwortliche eine gemeinsame Anwendung oder Verarbeitungsumgebung für einen gemeinsamen Wirtschaftssektor, ein bestimmtes Marktsegment oder für eine weit verbreitete horizontale Tätigkeit einführen möchten.

2.2.3. Positiv- und Negativlisten zur DSFA

Weiterer Prüfschritt zur Frage, ob eine Datenschutz-Folgenabschätzung vorzunehmen ist, werden in Zukunft die Positiv- bzw Negativlisten der Aufsichtsbehörden sein. Diese Listen definieren Verarbeitungsvorgänge, die jedenfalls einer DSFA bedürfen („Positivliste“), bzw solche, bei denen eine DSFA unterbleiben kann („Negativliste“). Beide Listen sind von den Aufsichts-behörden der Mitgliedstaaten dem Europäischen

2 Art-29-Datenschutzgruppe, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679, WP 248, angenommen am 4. 4. 2017, 7.

3 Art-29-Datenschutzgruppe, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679, WP 248, as last Revised and adopted on 4 October 2017 (rev.01).

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

Datenschutzausschuss im Rahmen des aufsichtsbehördlichen Kohärenzverfahrens zu übermitteln (Art 35 Abs 4), dies mit dem Ziel der Harmonisierung.

Anzumerken ist an dieser Stelle, dass die Artikel-29-Datenschutzgruppe in Fällen, in denen die Notwendigkeit einer Folgenabschätzung unklar ist, dennoch eine Durchführung empfiehlt, sei es auch nur als Hilfsmittel, um die datenschutzrechtlichen Vorgaben zu erfüllen.

2.3. Zeitpunkt der Durchführung einer DSFA

Die Wahl des Zeitpunkts der Durchführung einer DSFA, wie auch die Wahl der Methode, obliegt dem Verantwortlichen; die DSGVO gibt dazu keine weiteren Anhaltspunkte. Sanktioniert wird lediglich eine Nichtdurchführung. Empfehlenswert ist eine frühestmögliche Planung und Berücksichtigung der DSFA in Projekten. Die DSFA muss daher von jener Organisationseinheit (Fachabteilung etc) des Verantwortlichen angestoßen werden, die eine Verarbeitung plant. Es empfiehlt sich aus diesem Grund durch entsprechende Schulungen Bewusstsein in den Fachabteilungen zu schaffen, dass geplante Datenverarbeitungen möglicherweise eine DSFA erfordern.

Dem erhöhten bürokratischen Aufwand des Verantwortlichen wird so entgegengesetzt, dass Maßnahmen zur Risikominimierung im Projekt rechtzeitig berücksichtigt werden können.

Damit kann eine Datenschutz-Folgenabschätzung als Unterstützung bei der Lösungsfindung positioniert werden. Darüber hinaus ist die DSFA – wie erwähnt – auch ein Instrument zur effektiven und rechtzeitigen Umsetzung von Datenschutz durch Technikgestal-tung (Privacy by Design) und durch datenschutzfreundliche Voreinstellungen (Privacy by Default).

Bei entsprechend umfangreichen und aufwändigen Verarbeitungen wird sich die DSFA als Begleitung des Projektes über den gesamten Zeitraum von Idee und Konzeptionierung bis hin zur Implementierung und tatsächlichen Aufnahme der Verarbeitung erweisen. Damit wird der iterative Charakter der DSFA hervorgestrichen.

Nicht eindeutig zu beantworten ist die Frage, ob eine Pflicht zur Durchführung einer DSFA für Verarbeitungen besteht, die bereits vor Geltung der DSG-VO mit 25.5.2018 vorhanden waren. Geht man streng vom Wortlaut der Bestimmung aus („vorab“), ist eine DSFA nur

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

für solche Verarbeitungen durchzuführen, die nach dem 25.5.2018 aufgenommen werden bzw bei denen nach diesem Zeitpunkt eine signifikante Änderung eintritt.

Da die Verarbeitung bereits existiert, ist eine Vorab-Prüfung nicht mehr möglich. Zu berücksichtigen ist zudem, dass die existierenden Datenverarbeitungen nicht im „rechtsfreien Raum“ betrieben wurden (sofern der Verantwortliche die anwendbaren Rechtsvorschriften beachtet hat, ua betreffend Melde- bzw Vorabkontrolle).

Die Artikel-29-Datenschutzgruppe spricht jedoch eine dringende Empfehlung dafür aus, auch für bereits bestehende Verarbeitungen eine DSFA durchzuführen. Ebenfalls dafür sprechen in diesem Zusammenhang die bestehende Rechts-unsicherheit bzw die damit möglichen verbundenen Sanktionen.

2.4. Überprüfung der DSFA

Es ist in der Folge (nach Abschluss der Folgenabschätzung) nicht nur zu überprüfen, ob die vorgeschlagenen Maßnahmen tatsächlich umgesetzt wurden – erforderlichenfalls ist auch eine Überprüfung der Verarbeitung durchzuführen, um zu bewerten, ob hinsichtlich des mit den Verarbeitungsvorgängen verbundenen Risikos Änderungen eingetreten sind. Erwägungsgrund 89 sieht vor, dass bereits aufgrund der seit der ursprünglichen Verarbeitung vergangenen Zeit eine DSFA notwendig wird. Damit sollte bei der jeweils konkreten Datenschutz-Folgenabschätzung bereits mitbedacht werden bzw in der Dokumentation vermerkt werden, wann routinemäßig eine Überprüfung und gegebenenfalls Neudurchführung sinnvoll und angebracht ist.

Dabei sind die Entwicklung der Technologie, Änderungen bei den rechtlichen Gegebenheiten sowie Änderungen an der Art der Verarbeitung zu bedenken. Zusätzlich ist eine DSFA erneut durchzuführen, wenn sich ein Risiko verwirklicht.

Allgemein ist die Verpflichtung zur Durchführung der DSFA als Konkretisierung der Rechenschaftspflicht des Verantwortlichen zu sehen. Damit ergibt sich, dass in der Dokumentation und dem Bericht nicht nur die tatsächlich durchgeführte Folgenabschätzung dokumentiert wird, sondern es sollte darin auch festgehalten werden, warum eine DSFA nicht in Betracht gezogen wurde bzw nach einer Eingangsprüfung von einer Fortsetzung der Prüfung abgesehen wurde, obwohl zunächst zumindest ein Faktor für das Bestehen eines hohen Risikos für die Betroffenen identifiziert wurde.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

2.5. Konsultation der Aufsichtsbehörde gemäß Art 36 DSGVO

Weiterer und nicht unwesentlicher Faktor in der zeitlichen Planung der DSFA und insbesondere der tatsächlichen Aufnahme der Verarbeitung von Daten ist die allenfalls notwendige Konsultationspflicht der Aufsichtsbehörde. Der Verantwortliche hat die Aufsichtsbehörde zu konsultieren, wenn aus der DSFA hervorgeht, dass die Verarbeitung ein hohes Risiko zur Folge hätte, sofern der Verantwortliche keine Maßnahmen zur Eindämmung des Risikos trifft. Die Aufsichtsbehörde hat maximal vierzehn Wochen Zeit, auf die Konsultation zu reagieren. Bei einem entsprechend komplexen und neuartigen Projekt empfiehlt es sich daher, eine DSFA frühzeitig und zügig durchzuführen, um eine allfällige Konsultation der Aufsichtsbehörde im Projektplan berücksichtigen zu können.

3. WER HAT EINE DATENSCHUTZ-FOLGENABSCHÄTZUNG DURCHZUFÜHREN?

3.1. Grundlagen

Die Verantwortung für die Durchführung der DSFA liegt beim Verantwortlichen. Ursprünglich sah der Kommissionsentwurf vor, dass alternativ zum Verantwortlichen der in dessen Auftrag handelnde Auftragsverarbeiter eine Folgenabschätzung durchzuführen hatte. Demgegenüber findet sich jetzt in Erwägungsgrund 95 die Aussage, dass der Auftragsverarbeiter erforderlichenfalls den Verantwortlichen auf Anfrage bei der Gewährleistung der Einhaltung der sich aus der Durchführung der DSFA und der vorherigen Konsultation der Aufsichtsbehörde ergebenden Auflagen zu unterstützen hat.

In der Praxis wird es daher zweckmäßig sein, einen Auftragsverarbeiter, sofern vorhanden und bereits ausgewählt, vertraglich im Detail zur Mitwirkung und aktiven Unterstützung im gesamten Prozess der DSFA zu verpflichten. Dies ergibt sich auch aus Art 28 Abs 3 lit f, wonach der Vertrag über die Auftragsverarbeitung (bzw das andere Rechtsinstrument) vorzusehen hat, dass der Auftragsverarbeiter unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen den Verantwortlichen bei der Einhaltung der Verpflichtungen der Artikel 32 bis 36 unterstützt. Oft wird auch nur der Auftragsverarbeiter über die erforderlichen Informationen zur Beurtei-lung der in seiner Sphäre liegenden Aspekte der Verarbeitung verfügen. Dabei

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

wird die Gefahr der Offenlegung von Betriebs- und Geschäftsgeheimnissen ins Kalkül zu ziehen sein. Auch hier empfiehlt sich eine entsprechende vertragliche Regelung.

Ist eine Verarbeitung von Daten durch gemeinsame Verantwortliche vorgesehen, kann die DSFA iSd Art 35 Abs 1 S 2 auch durch einen der Verantwortlichen durchgeführt werden, wobei dies auf die Verantwortlichkeit der einzelnen Verantwortlichen keine Auswirkung hat.

3.2. Mitarbeit an der DSFA – wer soll einbezogen werden

Die DSFA sollte als Projekt organisiert werden und als solches von einer entsprechenden hohen Führungsebene mit den notwendigen materiellen und personellen Ressourcen ausgestattet werden. Bei der Zusammenstellung des Projektteams ist insbesondere auf die Komplexität des Projektes, die erforderlichen Fachkenntnisse und das erforderliche Wissen über das konkrete Projekt und dessen Umfeld zu achten. In der Praxis kann sich ein Team aus Juristen, Mitarbeitern der IT, CISO, Datenschutzbeauftragten, der Fachabteilung, die die Verarbeitung angefordert hat („data owner“) usw zusammensetzen. Ein besonderes Augenmerk liegt hier auf der Gewährleistung der Vermeidung von Interessenkonflikten. So sind diejenigen, die in der Zukunft mit der Verarbeitung von Daten befasst sind, nicht als unabhängig anzusehen, können anderseits aber wertvollen Input zur Ausgestaltung der Datenschutz-Folgenabschätzung liefern. Eine Durchführung kann sowohl durch ein internes Team, als auch durch externe Dritte geschehen. Idealerweise ist eine unabhängige Instanz zu beteiligen.

Der Verantwortliche hat den Rat des Datenschutzbeauftragten einzuholen, sofern er einen ernannt hat. Gemäß Art 39 Abs 1 lit c zählt die Beratung im Zusammenhang mit der DSFA und die Überwachung ihrer Durchführung zu den gesetzlichen Aufgaben des Datenschutzbeauftragten, dies jedoch nur auf Anfrage und nicht in federführender Stellung.

Es besteht also eine Verpflichtung des Verantwortlichen, den Rat des Datenschutz-beauftragten einzuholen. Zu welchem Zeitpunkt und mit welchem Anteil der Datenschutzbeauftragte in den Prozess eingebunden wird, liegt in der Entscheidung des Verantwortlichen. Ausreichend wäre auch eine nachträgliche Überprüfung des finalen Berichtes. In der Praxis wird die rechtzeitige Einbindung des Datenschutzbeauftragten, nicht zuletzt aufgrund seiner Fachkunde, dringend zu empfehlen sein.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

Abhängig von der Organisation des Verantwortlichen ist es empfehlenswert, die DSFA durch die Geschäftsleitung oder den dazu entsprechend bevollmächtigen Bereich abnehmen zu lassen.

4. WIE IST EINE DATENSCHUTZ-FOLGENABSCHÄTZUNG DURCHZUFÜHREN?

4.1. Grundlagen

Voranzustellen ist, dass die DSGVO keine bestimmte Form oder konkrete Methode der Ausgestaltung einer Datenschutz-Folgenabschätzung vorgibt und darüber auf nationaler und europäischer Ebene derzeit intensiv diskutiert wird. Die Artikel-29-Datenschutzgruppe führt ausdrücklich aus, dass unterschiedliche Ausgestaltungsmöglichkeiten bei der Unterstützung der Implementierung der Vorgaben der DSGVO Verwendung finden können und verweist auf Beispiele existierender (generischer bzw sektorspezifischer) DSFA-Verfahrensmodelle in Annex 1.[4]

4.2. Aufbau einer DSFA

Der Verantwortliche ist daher grundsätzlich frei, wie er den DSFA-Prozess durchführt und kann diesen an seine internen Verfahren anpassen, sofern er die in Art 35 Abs 7 DSGVO lit a bis d enthaltenen vier Anforderungen im Sinne von Mindestbestandteilen einer DSFA berücksichtigt, die die Artikel-29-Datenschutzgruppe in Annex 2 näher ausführt und zusätzlich um den Punkt „*interested parties are involved*“ (Beiziehung des Datenschutzbeauftragten [vgl Art 35 Abs 2] und Einbeziehung der Sichtweise der betroffenen Personen [vgl Art 35 Abs 9]) ergänzt:

4 Art-29-Datenschutzgruppe, WP 248, 15: Different methodologies (see Annex 1 for examples of data protection and privacy impact assessment methodologies) could be used to assist in the implementation of the basic requirements set out in the GDPR (Anm: Annex 1 findet sich auf Seite 20).

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

a) eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung, gegebenenfalls einschließlich der von dem Verantwortlichen verfolgten berechtigten Interessen;
b) eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck;
c) eine Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen gemäß Absatz 1 und
d) die zur Bewältigung der Risiken geplanten Abhilfemaßnahmen, einschließlich Garantien, Sicherheitsvorkehrungen und Verfahren, durch die der Schutz personenbezogener Daten sichergestellt und der Nachweis dafür erbracht wird, dass diese Verordnung eingehalten wird, wobei den Rechten und berechtigten Interessen der betroffenen Personen und sonstiger Betroffener Rechnung getragen wird.

4.3. Mindestinhalt einer DSFA

Art 35 Abs 7 lit a bis d DSGVO iVm den ErwGr 84 und 90 verlangt somit als Mindestinhalt:

1. eine systematische Beschreibung des gesamten Prüfgegenstands („target of evaluation“; eingebettet im Kontext, also nicht bloß der reinen Datenverarbeitung[en]) und des Verarbeitungszwecks,

2. eine Verhältnismäßigkeitsprüfung; in der Literatur auch als normative Bewertung der geplanten Datenverarbeitung betreffend deren Notwendigkeit und Verhältnismäßigkeit in Bezug auf den damit beabsichtigten Zweck, im Sinne einer Zweck-Mittel-Relation (über deren reine Zulässigkeit hinaus) umschrieben,

3. eine Risikobeurteilung (in der englischen Sprachfassung der DSGVO als „risk assessment“ bezeichnet; die Übersetzung als „Risikobewertung“, engl „risk evaluation“ greift zu kurz), die sich aus den drei Schritten

   3.1 Risikoidentifikation,

   3.2 Risikoanalyse (qualitative Kategorisierung nach Schwere des Risikos und dessen Eintrittswahrscheinlichkeit),

   3.3 Risikobewertung (zb mittels einer Risikomatrix) zusammensetzt; und

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

4. eine Risikobehandlung (Treffen von Maßnahmen zum Umgang mit den Risiken)

Die Punkte 3. und 4. sind dabei Ausprägungen des sog „risikobasierten Ansatz“ der DSGVO, welche nicht nur bei der Durchführung einer DSFA sondern auch im Kontext der Art 24, 25 und 32 DSGVO relevant sind. Mit anderen Worten ist die DSFA ein spezifisches Beispiel für den risikobasierten Ansatz bei Datenverarbeitungen, die (verkürzt gesprochen) ein voraussichtlich hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge haben, und nach einer umfangreicheren Risikobeurteilung und -behandlung verlangen. Grundsätzlich ist jedoch auch jeder anderen Zulässigkeitsprüfung einer Datenverarbeitung eine solche Risikoabschätzung samt adäquaten, risikominimierenden technischen und organisatorischen Maßnahmen vor deren Implementierung inhärent (vgl nur Art 24 Abs 1 DSGVO). *Wybitul/Ströbel/Sigel* empfehlen in diesem Zusammenhang auch in Fällen, die keine hohen Risiken zur Folge haben, eine (eingeschränkte oder angepasste) Folgenabschätzung zur Vermeidung von Bußgeldern, Schadenersatzforderungen und sonstigen Nachteilen durchzuführen.

4.4. Der Prozess einer Datenschutz-Folgenabschätzung

Die DSFA ist als Prozess (und nicht etwa nur als Bericht) zu betrachten, mit welchem ehestmöglich gestartet werden sollte, um die Gestaltung des Prüfgegenstands („Projekt“) beeinflussen zu können. Dadurch unterscheidet sich eine Folgenabschätzung auch von einem Audit, das ein Projekt ex post bewertet und für das „Einbacken“ der Datenschutzerfordernisse, welches das Ergebnis einer DSFA sein soll, üblicherweise zu spät kommt.

Es existieren mittlerweile zahlreiche Vorschläge für die Durchführung eines DSFA-Prozesses, welche in der einen oder anderen Weise den Ergebnissen der PIAF-Studie ähneln, in der 2012 für die EU-Kommission ua die Privacy Impact Assessment-Methodologien in sieben Staaten (samt Ableitung von „Best Practice“-Empfehlungen und

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

Kernbestandteilen eines Privacy Impact Assessment-Prozesses) untersucht wurden.[5] Folgende Kernelemente wurden dabei identifiziert:

1. Determining whether a PIA is necessary (threshold analysis),
2. Identifying the PIA team and setting terms of reference,
3. Description of the proposed project [and identification of stakeholders],
4. Analysis of the information flows and other privacy impacts,
5. Consultation with stakeholders,
6. Risks management [Identification of risks and possible solutions],
7. Legal compliance check,
8. Formulation of recommendations,
9. Preparation and publication of the report [e.g., on the organisation's website],
10. Implementation of recommendations,
11. External [Third-party] review and/or audit,
12. Revisiting PIA if the project in question changes [Updating the PIA if there are changes in the project]

Das Muster für die DSFA bei intelligenten Netzen und intelligenten Messsystemen, auf welches ausdrücklich in der Empfehlung 2014/724/EU der Europäischen Kommission verwiesen wird, sieht folgende Schritte vor:[6]

1. Step 1 - Pre-assessment and criteria determining the need to conduct a DPIA,
2. Step 2 - Initiation,
3. Step 3 - Identification, characterisation and description of smart grid systems / applications processing personal data,
4. Step 4 - Identification of relevant risks,
5. Step 5 - Data protection risk assessment,
6. Step 6 - Identification and recommendation of controls and residual risks,
7. Step 7 - Documentation and drafting of the DPIA Report,
8. Step 8 - Review and maintenance

5 *De Hert/Kloza/Wright* (Hrsg), PIAF, Recommendations for a privacy impact assessment framework for the European Union, Deliverable D3 (2012), http://piafproject.eu/ref/PIAF_D3_final.pdf; die weiteren Berichte sind unter http://piafproject.eu/Deliverables.html abrufbar.

6 Empfehlung 2014/724/EU der Kommission vom 10. Oktober 2014 über das Muster für die Datenschutz-Folgenabschätzung für intelligente Netze und intelligente Messsysteme, ABl L 2014/300, 63.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

Der neue Standard ISO/IEC 29134[7] enthält Leitlinien für einen Prozess zur Durchführung von Privacy Impact Assessments und für den Aufbau und Inhalt eines PIA-Berichts. Der Prozess wird dabei in folgende vier Unterprozesse gegliedert:

1. Threshold analysis (Schwellwertanalyse – Ermittlung der Notwendigkeit eines PIA),
2. Preparation of the PIA (Vorbereitung des PIA),
3. Perform the PIA (Durchführung des PIA) und
4. Follow-up of the PIA (Nachverfolgung des PIA)

In welche und wie viele Abschnitte man einen DSFA-Prozess unterteilt, ist primär Geschmackssache, weitere Vorschläge reichen beispielhaft von drei oder vier Phasen über sechs bis hin zu sieben Stufen. Wichtig ist uE vielmehr ein nachvollziehbarer Aufbau und Ablauf des Prozesses, der insbesondere die Vorgaben des Art 35 Abs 7 DSGVO und die Empfehlungen der Artikel-29-Datenschutzgruppe berücksichtigt. Siehe dazu das Muster für einen DSFA-Bericht in Anhang B der genannten Empfehlungen.

4.5. Die Einbindung betroffener Personen oder ihrer Vertreter

Gemäß Art 35 Abs 9 holt der Verantwortliche gegebenenfalls den Standpunkt der betroffenen Personen oder ihrer Vertreter zu der beabsichtigten Verarbeitung unbeschadet des Schutzes gewerblicher oder öffentlicher Interessen oder der Sicherheit der Verarbeitungsvorgänge ein. Durch die im Rahmen der Trilog-Verhandlungen erfolgte Einfügung des Worts „gegebenenfalls*“* besteht Unklarheit darüber, unter welchen Umständen konkret der Standpunkt Betroffener bzw ihrer Vertreter einzuholen ist und in welchen Fällen darauf (zulässigerweise) verzichtet werden kann. In der englischen Sprachfassung heißt es „where appropriate“, was auch als „angemessen“, „geeignet“ bzw „zweckdienlich“ übersetzt werden kann, die Artikel-29-Datenschutzgruppe geht in ihrer Stellungnahme auf diesen Begriff nicht näher ein. *Martini* lässt die Konsultationspflicht greifen, soweit Personengruppen (wohl im Sinn eines Betroffenenkreises) durch den (geplanten) Verarbeitungsvorgang in besonderer, identifizierbarer sowie adressierbarer Weise betroffen sind.

7 ISO/IEC 29134:2017 Information technology — Security techniques — Guidelines for privacy impact assessment (beschlossen im Juni 2017). Dieser Standard baut angeblich auf den Vorarbeiten der CNIL auf, siehe *Kranig/Sachs/Gierschmann*, Datenschutz-Compliance nach der DS-GVO (2017) 99.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

Die Art und Weise der Einholung der Stellungnahme ist kontextabhängig, die Artikel-29-Datenschutzgruppe anerkennt verschiedene Wege, so führt diese beispielhaft die (interne oder externe) Durchführung einer Studie, die formelle Befragung von Personalvertretern oder Gewerkschaften sowie die Übermittlung eines Fragebogens an die zukünftigen Kunden des Verantwortlichen an. Aus dem Wortlaut selbst lässt sich lediglich die Einholung des Standpunkts (in der urspr Fassung der Kommission „der Meinung“) ableiten, jedoch nicht die Pflicht zur Berücksichtigung oder gar eine über das ArbVG hinausgehende (neue) Zustimmungspflicht des Betriebsrats als Vertreter der Betroffenen. Dennoch wird sich der Verantwortliche mit den Ansichten der betroffenen Personen oder ihrer Vertreter auseinandersetzen und in der Folgenabschätzung darauf einzugehen haben. Ob dabei auch Verbraucher(schutz)verbände unter den Begriff des Vertreters subsumiert werden können, ist in der Lit strittig.[8] Jedenfalls lässt die Konsultationspflicht expressis verbis den Schutz gewerblicher oder öffentlicher Interessen oder der Sicherheit der Verarbeitungsvorgänge unberührt, dh der Verantwortliche kann die aus Art 35 Abs 9 erwachsende Informationspflicht über die beabsichtigte Verarbeitung gegenüber den betroffenen Personen bzw Vertretern im verhältnismäßigen Ausmaß einschränken bzw in extremis verweigern (was im letzteren Fall dazu führen wird, dass a priori keine Einbindung iSd Art 35 Abs 9 erfolgen können wird, ist doch das Vorliegen von ausreichenden Informationen conditio sine qua non für die Meinungsbildung durch die betroffenen Personen oder ihrer Vertreter).

Für die Durchführung der Datenschutz-Folgenabschätzung ist es empfehlenswert, im Bericht zu Nachweiszwecken zu dokumentieren, warum kein oder nur ein inhaltlich beschränkter Standpunkt eingeholt wurde bzw der eingeholte Standpunkt nicht oder nur teilweise Berücksichtigung gefunden hat.

4.6. Der Bericht über die Durchführung einer Datenschutz-Folgenabschätzung

Bereits an dieser Stelle sei angemerkt, dass der DSFA-Bericht nicht das eigentliche Ziel einer DSFA ist, sondern ein „Mittel zum Zweck“ um den Prozess (nach innen und außen) dokumentieren zu können. Dabei soll und darf die Berichterstellung nicht unterschätzt

8 Dafür *Martini* in Paal/Pauly (Hrsg), Datenschutz-Grundverordnung (2016) Art 35 Rz 60; dagegen (mangels rechtlicher Verbundenheit) *Laue/Nink/Kremer*, Das neue Datenschutzrecht in der betrieblichen Praxis (2016) 245 Rz 99.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

werden – dieser hält ja die Durchführung und die Ergebnisse fest, wobei ein bloßer „Marketing-DSFA-Bericht“ schon aus Gründen der Compliance zu vermeiden ist. Der Bericht kann zugleich als Handlungsanweisung und Checkliste bei der Durchführung der DSFA dienen.

Art 35 DSGVO enthält – etwas überraschend – keine explizite Vorschrift, wonach über die Durchführung einer DSFA ein Bericht zu erstellen ist. Dass jedoch eine Dokumentationspflicht des Verantwortlichen besteht, ist nach Auffassung der Verfasser unzweifelhaft und ergibt sich einerseits implizit bereits aus Art 35 Abs 7 DSGVO, zudem aus Art 5 Abs 2 DSGVO (Rechenschaftspflicht) iVm Art 24 Abs 1 DSGVO und Art 36 Abs 3 lit e (wonach der Aufsichtsbehörde „die Datenschutz-Folgenabschätzung gemäß Artikel 35“ zur Verfügung zu stellen ist). Auch die von Art 35 Abs 11 geforderte Überprüfung zur Bewertung, ob die Verarbeitung gemäß der DSFA durchgeführt wird, setzt ein Festhalten der Ergebnisse der Folgenabschätzung voraus. Darüber hinaus entspricht die Berichterstellung über durchgeführte PIAs der weltweiten „Good Practice“ in diesem Bereich (siehe dazu unten Abschnitt IV.1.), auf welcher die in Art 35 DSGVO vorgesehene DSFA offensichtlich aufbaut.

Zu empfehlen ist eine parallele Begleitung des DSFA-Prozesses im Sinne eines „living document“ beginnend bereits mit der Dokumentation der Schwellwertanalyse, also der Ermittlung der Notwendigkeit der Durchführung einer DSFA. Selbst wenn diese Analyse ergeben sollte, dass eine DSFA nicht erforderlich ist und der Prozess somit abgebrochen wird, kommt damit der Verantwortliche seiner Rechenschafts- und Nachweispflicht nach. Diese schriftliche Dokumentation kann in einem etwaigen künftigen Verfahren der Aufsichtsbehörde vorgelegt werden und zeichnet die internen Überlegungen und Einschätzungen nach.

Inhaltlich hält der DSFA-Bericht im Wesentlichen den Ablauf (samt Sachverhaltsdarstellung im Sinne einer systematischen Beschreibung des gesamten Prüfgegenstands - „target of evaluation“) und die Ergebnisse des DSFA-Prozesses fest. Wie bereits für den DSFA-Prozess selbst gilt auch hier, dass die DSGVO keine spezifischen Vorschriften für die Ausgestaltung eines DSFA-Berichts vorsieht. Als Mindestinhalte sind jedoch die von der Artikel-29-Datenschutzgruppe in Annex 2 des WP 248 angeführten Kriterien, welche im Wesentlichen auf Art 35 Abs 7 beruhen, vorgezeichnet. Die ISO/IEC 29134 empfiehlt folgende Inhalte des Berichts über ein Privacy Impact Assessment, wobei der Schwerpunkt auf der Risikobeurteilung liegt:

1. relevante Datenschutzanforderungen
2. Beschreibung des Umfangs

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

3. verwendete Risikokriterien
4. Beteiligte bei der Durchführung
5. konsultierte Stakeholder

Für diese Schwerpunktsetzung spricht auch ErwGr 90, worin ua wie folgt ausgeführt wird: „Diese Folgenabschätzung sollte sich insbesondere mit den Maßnahmen, Garantien und Verfahren befassen, durch die dieses Risiko eingedämmt, der Schutz personenbezogener Daten sichergestellt und die Einhaltung der Bestimmungen dieser Verordnung nachgewiesen werden soll."

In der sehr detaillierten PIAF-Studie wird als Mindestinhalt eines PIA-Berichts Folgendes angeführt: [9]

1. introduction and background information including who undertook the PIA, her contact details and where to find further information and other sources of help and advice;
2. a description of the project, of the information flows and of the impacts on privacy;
3. results of the consultation of stakeholders;
4. description of the risk assessment and risk mitigation phases, including the alternatives considered;
5. analysis of legal compliance;
6. recommendations;
7. annexes, if necessary

Liegt der Bericht bzw ein finaler Entwurf vor, kann sich die Frage stellen, was damit beim Verantwortlichen (intern) zu geschehen hat, vor allem ob und von wem dieser „abzuzeichnen" ist – ein praktisch relevanter Punkt über den sich die DSGVO ausschweigt. Die ICO sieht in ihrem Code of Practice ausdrücklich folgenden Punkt vor: "Obtain appropriate signoff within the organization".[10] Da der Verantwortliche die DSFA durchzuführen hat, ist es auch nachvollziehbar, dass entsprechend autorisierte Vertreter

9 *De Hert/Kloza/Wright* (Hrsg), PIAF, Recommendations for a privacy impact assessment framework for the European Union, Deliverable D3 (2012) 31, http://piafproject.eu/ref/PIAF_D3_final.pdf.

10 ICO, Conducting privacy impact assessments code of practice (2014) 13, https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

des Verantwortlichen in die DSFA eingebunden sind und auch die Letztverantwortung zu tragen haben. Die Leitungsebene wird üblicherweise die letzte Entscheidungshoheit über das Ob und Wie des der DSFA unterzogenen Projekts zukommen. Als Minimalvariante sollte die Projektleitung bzw der Datenschutzbeauftragte der „höchsten Managementebene“ Bericht erstatten, wie dies Art 38 Abs 3 DSGVO vorsieht.

Die DSGVO kennt keine Verpflichtung zur Veröffentlichung der DSFA, die Artikel-29-Datenschutzgruppe empfiehlt jedoch deren (zumindest teilweise) Veröffentlichung, um das Vertrauen in die Datenverarbeitung zu stärken und Transparenz zu leben. Insbesondere wird eine Veröffentlichung in Fällen angeregt, in denen ein Teil der Öffentlichkeit von der (geplanten) Verarbeitung betroffen sein wird.

5. SCHLUSSFOLGERUNGEN UND PRAXISTIPS

Besonders die Aufsichtsbehörden mit guter Ressourcenausstattung haben über die Jahre eigene Ansätze zur Durchführung von Privacy Impact Assessments entwickelt. Es ist aus heutiger Sicht zu erwarten, dass diejenigen Datenschutzbehörden, welche bereits ein eigenes Modell entwickelt haben, dieses bevorzugen bzw propagieren werden, nicht zuletzt deswegen, da die Kenntnis bei der jeweiligen Aufsichtsbehörde über die eigenen Empfehlungen am ausgeprägtesten sein wird. Die Inhalte der derzeit vorliegenden Modelle nationaler Aufsichtsbehörden (aus EU-Mitgliedsstaaten) stammen dabei oft-mals aus der Zeit vor Inkrafttreten der DSGVO und sind (noch) nicht durchgehend an die Vorgaben bzw die Terminologie der DSGVO angepasst.

Die ICO hat ihren aus 2014 stammenden PIA Code of Practice jedoch zuletzt Anfang 2017 im (lesenswerten) Bericht über „Big data, artificial intelligence, machine learning and data protection“ um die Anforderungen bzw die Terminologie der DSGVO ergänzt was auch von den anderen Datenschutzbehörden zu er-warten ist. Abzuwarten bleibt zudem, ob der Europäische Datenschutzausschuss (Art 68) Leitlinien, Empfehlungen und/oder bewährte Verfahren für DSFA gem Art 70 Abs 1 lit e bereitstellen wird.

Empfehlungen im Überblick:

- Dokumentation aller Entscheidungen, insbesondere warum ggf. keine Datenschutz-Folgenabschätzung durchgeführt wurde
- Im Zweifel Durchführung einer Datenschutz-Folgenabschätzung

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

- Einbeziehung der internen und externen Betroffenen
- Heranziehen von Mustern, Best Practices und ggf. ähnlichen, bereits durchgeführten Datenschutz-Folgenabschätzungen
- Veröffentlichen der Datenschutz-Folgenabschätzung
  - Insbesondere durch öffentliche Stellen
  - Zeigt Datenschutz-Bewusstsein und schafft Vertrauen

6. EXTERNE QUELLEN & WEBLINKS

6.1. Bücher

- Voigt, P., von dem Bussche, A., The EU General Data Protection Regulation (GDPR) – A Practical Guide, Springer International Publishing (2017);
- Boardman, R., Mullock, J., Mole, A. Bird & Bird Guide to General Data Protection Regulation (2016);
- EU General Data Protection Regulation (GDPR). An Implementation and Compliance Guide, IT Governance Publishing, Cambridgeshire (2016);
- European Data Protection. Law and Practice, Executive Editor: Edurado Ustaran, CIPP/E, Partner, Hogan Lovells, IAPP (2018);

6.2. Dokumente der Artikel 29 Working Party

- WP29, Guidelines on Consent under Regulation 2016/679, WP 259;
- WP29, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, WP 217;

6.3. Web Links

- http://europa.eu/rapid/press-release_IP-18-386_en.htm
- https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en
- https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/grounds-processing/when-can-personal-data-be-processed_en

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

- https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/grounds-processing/what-does-grounds-legitimate-interest-mean_en
- https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/grounds-processing/when-consent-valid_en
- https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/grounds-processing/does-consent-given-25-may-2018-continue-be-valid-once-gdpr-starts-apply-25-may-2018_en
- https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/grounds-processing/what-if-somebody-withdraws-their-consent_en
- https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/grounds-processing/what-if-somebody-withdraws-their-consent_en

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

ProLegis

TRANSPARENZ

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

Dissemination Level:		
PU	Public	
CO	Confidential, only for members of the consortium (including the Commission Services)	
EU-RES	Classified Information: RESTREINT UE (Commission Decision 2005/444/EC)	
EU-CON	Classified Information: CONFIDENTIEL UE (Commission Decision 2005/444/EC)	
EU-SEC	Classified Information: SECRET UE (Commission Decision 2005/444/EC)	
Document version control:		
Version	**Author(s)**	**Date**
Version 1	Developed by:	
Version 1	Reviewed & updated by:	
Version 2	Translated by: VICESSE	21/06/18

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

Inhaltsverzeichnis

1. RECHTLICHER RAHMEN 5
1.1. Europäische Verträge 5
1.2. Charta der Grundrechte der EU 5
1.3. DSGVO 6
2. BEDEUTUNG DER TRANSPARENZ IN DER DSGVO 7
2.1. Elemente der Transparenz im Rahmen der DSGVO (Art. 12) 8
2.1.1. “Prägnant, transparent, verständlich und leicht zugänglich” 8
2.1.2. “Klare und klare Sprache” 9
2.1.3. Art der Informationsbereitstellung (Art. 12 Abs. 1 & Abs. 5 "kostenlos"). ... 9
2.2. Informationen für die betroffenen Personen (Art. 13 und Art. 14) 10
2.2.1. Welche Informationen sollten zur Verfügung gestellt werden? 10
2.2.2. Welche zusätzlichen Informationen sollten bereitgestellt werden? 10
2.2.3. Wie sollten die Informationen bereitgestellt werden? 11
2.2.4. Wann sollen Informationen bereitgestellt werden? 12
2.2.5. Wann sollten bei Änderungen der Transparenz Informationen gemeldet werden, die von den Verantwortlichen bereitgestellt werden sollen? 13
2.3. Modalitäten 13
2.3.1. Datenschutzhinweise 13
2.3.2. “Push” & “pull” Notifikationen 14
2.3.3. Andere Arten von "geeigneten Maßnahmen" 14
2.3.4. Visualisierungen 15
2.4. Ausübung der Rechte von Datensubjekten 15
2.4.1. Ausnahmen von der Informationspflicht 15
3. SCHLUSSFOLGERUNG & PRAKTISCHE HINWEISE 16
4. EXTERNE QUELLEN & WEBLINKS 17
4.1. Bücher 17
4.2. Dokumente der Artikel 29 Working Party 17

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

4.3. Web Links 17
5. REFERENZEN 18

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

1. RECHTLICHER RAHMEN

1.1. Europäische Verträge

Treaty of the European Union (Maastrich)

Artikel 1 TEU: Dieser Vertrag stellt eine neue Stufe bei der Verwirklichung einer immer engeren Union der Völker Europas dar, in der die Entscheidungen möglichst offen und möglichst bürgernah getroffen werden.

Artikel 11(2) TEU: Die Organe pflegen einen offenen, transparenten und regelmä-ßigen Dialog mit den repräsentativen Verbänden und der Zivilgesellschaft.

Treaty on the Fuctioning of the European Union (Rome)

Artikle 15 (2) TFEU: Jeder Unionsbürger sowie jede natürliche oder juristische Person mit Wohnsitz oder satzungsgemäßem Sitz in einem Mitgliedstaat hat das Recht auf Zugang zu Dokumenten der Organe, Einrichtungen und sonstigen Stellen der Union, unabhängig von der Form der für diese Dokumente verwendeten Träger, vorbehaltlich der Grundsätze und Bedingungen, die nach diesem Absatz festzulegen sind.

1.2. Charta der Grundrechte der EU

Transparenz ist ein wesentliches Element des Grundsatzes der fairen Verarbeitung. Eine solche Transparenz ist in Artikel 8 der Charta der Grundrechte der EU enthalten.

Artikel 8

Schutz personenbezogener Daten

(1) Jede Person hat das Recht auf Schutz der sie betreffenden personenbezoge-nen Daten.

(2) Diese Daten dürfen nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

Grundlage verarbeitet wer- den. Jede Person hat das Recht, Auskunft über die sie betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu erwirken.

(3) Die Einhaltung dieser Vorschriften wird von einer unabhängigen Stelle überwacht.

1.3. DSGVO

Artikel 5

Grundsätze für die Verarbeitung personenbezogener Daten

1. Personenbezogene Daten müssen

a) auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden („Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz“);

Erwägungsgründe

(39) Jede Verarbeitung personenbezogener Daten sollte rechtmäßig und nach Treu und Glauben erfolgen. Für natürliche Personen sollte Transparenz dahingehend bestehen, dass sie betreffende personenbezogene Daten erhoben, verwendet, eingesehen oder anderweitig verarbeitet werden und in welchem Umfang die personenbezogenen Daten verarbeitet werden und künftig noch verarbeitet werden. Der Grundsatz der Transparenz setzt voraus, dass alle Informationen und Mitteilungen zur Verarbeitung dieser personenbezogenen Daten leicht zugänglich und verständlich und in klarer und einfacher Sprache abgefasst sind. Dieser Grundsatz betrifft insbesondere die Informationen über die Identität des Verantwortlichen und die Zwecke der Verarbeitung und sonstige Informationen, die eine faire und transparente Verarbeitung im Hinblick auf die betroffenen natürlichen Personen gewährleisten, sowie deren Recht, eine Bestätigung und Auskunft darüber zu erhalten, welche sie betreffende personenbezogene Daten verarbeitet werden. Natürliche Personen sollten über die Risiken, Vorschriften, Garantien und Rechte im Zusammenhang mit der Verarbeitung personenbezogener Daten informiert und darüber aufgeklärt werden, wie sie ihre diesbezüglichen Rechte geltend machen können. Insbesondere sollten die bestimmten Zwecke, zu denen die personenbezogenen Daten verarbeitet werden, eindeutig und rechtmäßig sein und zum Zeitpunkt der Erhebung der

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

personenbezogenen Daten feststehen. Die personenbezogenen Daten sollten für die Zwecke, zu denen sie verarbeitet werden, angemessen und erheblich sowie auf das für die Zwecke ihrer Verarbeitung notwendige Maß beschränkt sein. Dies erfordert insbesondere, dass die Speicherfrist für personenbezogene Daten auf das unbedingt erforderliche Mindestmaß beschränkt bleibt. Personenbezogene Daten sollten nur verarbeitet werden dürfen, wenn der Zweck der Verarbeitung nicht in zumutbarer Weise durch andere Mittel erreicht werden kann. Um sicherzustellen, dass die personenbezogenen Daten nicht länger als nötig gespeichert werden, sollte der Verantwortliche Fristen für ihre Löschung oder regelmäßige Überprüfung vorsehen. Es sollten alle vertretbaren Schritte unternommen werden, damit unrichtige personenbezogene Daten gelöscht oder berichtigt werden. Personenbezogene Daten sollten so verarbeitet werden, dass ihre Sicherheit und Vertraulichkeit hinreichend gewährleistet ist, wozu auch gehört, dass Unbefugte keinen Zugang zu den Daten haben und weder die Daten noch die Geräte, mit denen diese verarbeitet werden, benutzen können.

(58) Der Grundsatz der Transparenz setzt voraus, dass eine für die Öffentlichkeit oder die betroffene Person bestimmte Information präzise, leicht zugänglich und verständlich sowie in klarer und einfacher Sprache abgefasst ist und gegebenenfalls zusätzlich visuelle Elemente verwendet werden. Diese Information könnte in elektronischer Form bereitgestellt werden, beispielsweise auf einer Website, wenn sie für die Öffentlichkeit bestimmt ist. Dies gilt insbesondere für Situationen, wo die große Zahl der Beteiligten und die Komplexität der dazu benötigten Technik es der betroffenen Person schwer machen, zu erkennen und nachzuvollziehen, ob, von wem und zu welchem Zweck sie betreffende personenbezogene Daten erfasst werden, wie etwa bei der Werbung im Internet. Wenn sich die Verarbeitung an Kinder richtet, sollten aufgrund der besonderen Schutzwürdigkeit von Kindern Informationen und Hinweise in einer dergestalt klaren und einfachen Sprache erfolgen, dass ein Kind sie verstehen kann.

2. BEDEUTUNG DER TRANSPARENZ IN DER DSGVO

Der Grundsatz der Transparenz ist mit den Grundsätzen der Fairness und Rechenschaftspflicht verknüpft. Artikel 5 (Grundsätze in Bezug auf die Verarbeitung personenbezogener Daten) verpflichtet die für die Verarbeitung Verantwortlichen, nachzuweisen, dass personenbezogene Daten in transparenter Weise verarbeitet werden. Gemäß Artikel 29 Datenschutzgruppe[i] zielt die Transparenz darauf ab, die betroffenen Personen zu befähigen, Verantwortliche der Verarbeitung und Datenverarbeiter zur Rechenschaft zu ziehen und die Kontrolle über ihre personenbezogenen Daten auszuüben.[ii] Dieses Ziel

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

wird durch die Einführung spezifischer praktischer Anforderungen erreicht, die in allen Verarbeitungsstufen zu beachten sind: vor oder zu Beginn der Datenverarbeitung, wenn die personenbezogenen Daten erhoben werden, und während der gesamten Bearbeitungszeit.

2.1. Elemente der Transparenz im Rahmen der DSGVO (Art. 12)

2.1.1. “Prägnant, transparent, verständlich und leicht zugänglich”

Die ersten beiden Teile dieser Anforderung bedeuten, dass die für die Datenverarbeitung Verantwortlichen die Informationen / Kommunikation effizient und kurz präsentieren sollten, um eine Informationsermüdung zu vermeiden (oder andernfalls die betroffenen Personen mit Informationen zu überschwemmen). Ein Weg, um dies zu tun, können mehrfache Mitteilungen sein, bei denen die Teilnehmer Schritt für Schritt über ihre Rechte informiert werden (zum Beispiel die Schlüsselinformationen in kurzer Zeit und den Rest - zum Zeitpunkt der Datenerhebung). Diese Informationen sollten getrennt von anderen nicht datenschutzrelevanten Informationen wie Vertragsbestimmungen sein.

Die Anforderung, dass Information "verständlich" ist, bedeutet, dass sie von einem durchschnittliches Mitglied der beabsichtigten Zielgruppe verstanden werden sollte, im aktuellen Fall vom durchschnittlichen Bürger der lokalen Gemeinschaft. Die betroffenen Personen sollten im Voraus bestimmen können, was der Umfang und die Folgen der Verarbeitung sind. Die Artikel 29 Arbeitsgruppe (WP29) rät, dass Datenverantwortliche in eindeutiger Sprache darlegen, welche die wichtigsten Konsequenzen der Verarbeitung sein werden, insbesondere wenn solche Konsequenzen Auswirkungen auf die Grundrechte der Subjekte haben können.[iii]

Das Element "leicht zugänglich" bedeutet, dass die betroffene Person nicht die Informationen suchen muss. Stattdessen sollte es in einer offensichtlichen Weise präsentiert werden, so dass das Subjekt ohne Anstrengung auf es zugreifen kann.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

2.1.2. “Klare und klare Sprache”

Die Forderung nach klarer und verständlicher Sprache bedeutet, dass Informationen so einfach wie möglich zur Verfügung gestellt werden sollten, um komplexe Satz- und Sprachstrukturen zu vermeiden. Die Informationen sollten nicht abstrakt oder ambivalent formuliert sein oder Raum für unterschiedliche Interpretationen lassen.[iv] Die Zwecke und die Rechtsgrundlage für die Verarbeitung personenbezogener Daten sollten klar sein. Eine unklare Formulierung der Verarbeitungszwecke wie "für die Entwicklung zukünftiger Dienste" von "für Forschungszwecke" soll vermieden werden. Die einer betroffenen Person zur Verfügung gestellten Informationen sollten keine übermäßig legalistische, technische oder fachspezifische Sprache oder Terminologie enthalten[v].

Die lokalen Behörden sollten außerdem sicherstellen, dass das Vokabular, der Ton und der Stil der Sprache, die bei der Ansprache von Kindern verwendet wird, für Kinder geeignet ist, so dass sie erkennen, dass die Nachricht / Information an sie gerichtet ist[vi].

2.1.3. Art der Informationsbereitstellung (Art. 12 Abs. 1 & Abs. 5 "kostenlos").

Die für die Verarbeitung Verantwortlichen dürfen den betroffenen Personen zur Bereitstellung von Informationen nach den Artikeln 13 und 14 (Informationen an die betroffene Person) oder nach den Artikeln 15 - 22 (Rechte betroffener Personen) und Artikel 34 (Mitteilung von Verletzungen personenbezogener Daten gegenüber betroffenen Personen) keine Kosten verursachen. Es gibt eine Ausnahme von dieser Regel: wenn Anfragen einer betroffenen Person offensichtlich unbegründet oder übermäßig sind, insbesondere wegen ihres sich wiederholenden Charakters. In diesem Fall kann der für die Verarbeitung Verantwortliche eine angemessene Gebühr erheben, die die Verwaltungskosten für die Bereitstellung der Informationen oder Mitteilungen oder die Durchführung der angeforderten Maßnahmen berücksichtigt. Es ist wichtig, dass die für die Datenverarbeitung Verantwortlichen wissen, dass sie die Beweislast für den offensichtlich unbegründeten oder übermäßigen Charakter des Antrags tragen müssen. Daher ist es nicht ratsam, dass die lokalen Behörden den Bürgern die Bereitstellung von Informationen im Rahmen der DSGVO in Rechnung stellen.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

2.2. Informationen für die betroffenen Personen (Art. 13 und Art. 14)

2.2.1. Welche Informationen sollten zur Verfügung gestellt werden?

Die Artikel 13 und 14 der DSGVO legen fest, welche Informationen der betroffenen Person zur Verfügung gestellt werden müssen. Die Verordnung unterscheidet zwischen Fällen, in denen die Information von der betroffenen Person stammt (Art. 13), und Fällen, in denen dies nicht der Fall ist (Art. 14). Die lokalen Behörden sollten Folgendes bereitstellen:

1. Informationen über ihre Identität, einschließlich ihrer Kontaktinformationen;
2. Kontaktdaten des Datenschutzbeauftragten;
3. Zwecke der Verarbeitung und ihrer Rechtsgrundlage - meist für lokale Behörden wäre dies Art. 6, Abs. 1 lit. e) Ausübung öffentlicher Gewalt, die dem für die Verarbeitung Verantwortlichen übertragen wurde, und die entsprechenden Bestimmungen der Rechtsvorschriften des Mitgliedstaats;
4. die Art der Daten, die verarbeitet werden, wenn sie nicht von der betroffenen Person zur Verfügung gestellt wurden;
5. die Identität der möglichen Empfänger der Daten - dies schließt nicht nur Dritte, sondern auch Verarbeiter und gemeinsame Verantwortliche („joint controllers“) ein. Der Verantwortlcihe sollte so spezifisch wie möglich sein, wenn die verschiedenen Kategorien von Datenempfängern definiert werden.

2.2.2. Welche zusätzlichen Informationen sollten bereitgestellt werden?

Um eine faire und transparente Verarbeitung zu gewährleisten, muss der für die Verarbeitung Verantwortliche der betroffenen Person Folgendes zur Verfügung stellen:

1. der Zeitraum, für den die persönlichen Daten gespeichert werden, oder die Kriterien, die für die Bestimmung dieses Zeitraums verwendet wurden;
2. das Bestehen des Rechts, von dem für die Verarbeitung Verantwortlichen Zugang, Berichtigung oder Löschung personenbezogener Daten zu verlangen, oder Einschränkung der Verarbeitung bezüglich der betroffenen Person oder der Verarbeitung zu widersprechen sowie das Recht auf Datenübertragbarkeit;

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

3. wenn die Verarbeitung auf Zustimmung beruht, das Bestehen des Widerrufsrechts
4. Zustimmung zu jeder Zeit;
5. das Recht, eine Beschwerde bei einer Aufsichtsbehörde einzureichen;
6. das Vorhandensein einer automatisierten Entscheidungsfindung einschließlich Profiling und aussagekräftiger Informationen über die dahinterstehende Logik sowie die Bedeutung und die beabsichtigten Konsequenzen einer solchen Verarbeitung für die betroffene Person.

Die Informationen über das Profiling sollten nicht nur für die betroffenen Personen leicht zugänglich sein, sondern müssen ihnen zur Kenntnis gebracht werden. Der Verantwortliche sollte einfache Wege finden, dem Betroffenen die Logik oder die Kriterien für die automatisierte Entscheidungsfindung ohne komplexe Erklärungen der Algorithmen mitzuteilen.

Wenn die Daten nicht von der betroffenen Person erhalten wurden, sollte der für die Verarbeitung Verantwortliche ihre Quelle angeben. Wenn die betroffene Person die Daten zur Verfügung stellt, sollte der für die Verarbeitung Verantwortliche sie informieren, wenn die Bereitstellung personenbezogener Daten gesetzlich vorgeschrieben ist.

Zweitens sollten die für die Verarbeitung Verantwortlichen die betroffenen Personen informieren, wenn sie beabsichtigen, die Daten für andere Zwecke als die, für die die Daten erhoben wurden, zu verarbeiten. Die betroffenen Personen müssen Informationen über diesen anderen Zweck und über alle relevanten weiteren Informationen erhalten, die mit den für den ursprünglichen Zweck bereitgestellten Informationen identisch sind (Verarbeitungszeitraum, Rechtsgrundlage für die Verarbeitung usw.). Bei der Datenerhebung könnte es nützlich sein, die betroffenen Personen über eine eventuelle künftige Verarbeitung zu informieren, wenn dies wahrscheinlich aufgrund der Tätigkeit des für die Verarbeitung Verantwortlichen geschieht.

2.2.3. Wie sollten die Informationen bereitgestellt werden?

Die Bereitstellung von Informationen und die Kommunikation mit betroffenen Personen erfolgt standardmäßig schriftlich. Die DSGVO ermöglicht jedoch auch die Bereitstellung von Informationen auf anderem Wege, einschließlich elektronischer Daten. Gemäß der WP29 ist es entscheidend, dass die Methoden, die für die Bereitstellung der Informationen ausgewählt wurden, den jeweiligen Umständen angepasst sind.[vii] Informationen können einer betroffenen Person auf Anfrage mündlich übermittelt werden, wenn ihre

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

Identitätsinformationen durch andere (d.h. nicht-verbale) Mittel nachgewiesen werden. Es gibt eine Ausnahme von dieser Regel bezüglich der Informationen, die die für die Verarbeitung Verantwortlichen gemäß Art. 13 und 14 verarbeitet - diese Information sollten dem Betroffenen ohne Identitätsprüfung mitgeteilt werden. Die mündliche Bereitstellung von Informationen bedeutet nicht notwendigerweise mündliche Informationen, die von Person zu Person bereitgestellt werden, sondern könnte auch eine automatisierte mündliche Information bedeuten. Laut WP29 sollte der für die Datenverarbeitung Verantwortliche der betroffenen Person erlauben, aufgezeichnete Nachrichten erneut zu hören, insbesondere wenn es sich um sehbehinderte Datensubjekte oder andere betroffene Personen handelt, die Schwierigkeiten haben, Informationen in schriftlicher Form zu erhalten oder zu verstehen. Im Falle der mündlichen Übermittlung von Informationen sollten die für die Verarbeitung Verantwortlichen auch nachweisen können, dass sie die Anforderungen der DSGVO erfüllt haben. Zu diesem Zweck sollten sie die folgenden Aspekte sicherstellen: 1) die Anforderung der Informationen auf mündlichem Wege, 2) die Art und Weise, mit der die Identität der betroffenen Person verifiziert wurde, und 3) die Tatsache, dass die Daten zur Verfügung gestellt wurden[viii].

2.2.4. Wann sollen Informationen bereitgestellt werden?

Informationen über die Verarbeitung personenbezogener Daten sind der betroffenen Person zum Zeitpunkt der Sammlung mitzuteilen (Art. 13 Abs. 1). Wenn Daten nicht direkt von der betroffenen Person, sondern von einer anderen Quelle stammen, werden die Informationen der betroffenen Person innerhalb einer angemessenen Frist, spätestens jedoch innerhalb eines Monats nach Erhalt, in Abhängigkeit von den Umständen des Falles zur Verfügung gestellt. Es gibt zwei spezifische Fälle: Erstens, wenn die Daten für die Kommunikation mit dem Subjekt verwendet werden, sollten die Informationen spätestens zum Zeitpunkt der ersten Kommunikation mit diesem Subjekt bereitgestellt werden; und zweitens, wenn erwartet wird, dass die Daten einem anderen Empfänger spätestens bei der ersten Weitergabe an diesen Empfänger offengelegt werden.

Dieser Zeitraum kann aufgrund der Komplexität und Anzahl der Anfragen (z.B. wenn die Anfrage mehrere Datenbanken umfasst) auf maximal drei Monate verlängert werden. Der für die Verarbeitung Verantwortliche muss die betroffene Person innerhalb eines Monats nach Erhalt des Antrags über die Verlängerung informieren, zusammen mit den Gründen für die Verspätung und Informationen über die Rechte des Antragstellers, eine Beschwerde einzureichen.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

2.2.5. Wann sollten bei Änderungen der Transparenz Informationen gemeldet werden, die von den Verantwortlichen bereitgestellt werden sollen?

In Situationen in denen die Änderung der Informationen schwerwiegende Auswirkungen auf die betroffene Person haben könnte, sollten die für die Verarbeitung Verantwortlichen rechtzeitig vor Inkrafttreten der Änderung Informationen bereitstellen. Dies sollte in einer expliziten und effektiven Weise geschehen.[ix] Die Bürger sollten genügend Zeit haben, um über die Art und die Auswirkungen der Änderung nachzudenken und ihre Rechte im Rahmen der Datenschutz-Grundverordnung in Bezug auf die Änderung auszuüben, um beispielsweise der Verarbeitung zu widersprechen. Die WP29 empfiehlt, die betroffenen Personen regelmäßig an den Umfang der Datenverarbeitung zu erinnern[x].

Bei der Planung der Verarbeitung der Daten zu einem anderen Zweck als dem, für den sie erhalten wurden, sollten die betroffenen Personen informiert werden, bevor die neue Verarbeitung begonnen hat.

2.3. Modalitäten

Modalitäten sind die Formate, in denen die für die Verarbeitung Verantwortlichen ihren Verpflichtungen im Rahmen der Datenschutz-Grundverordnung nachkommen, den betroffenen Personen Informationen zur Verfügung zu stellen.

2.3.1. Datenschutzhinweise

In Bezug auf Online-Plattformen empfiehlt es sich mehrfache Datenschutzerklärungen / -hinweise zu verwenden, um eine Verknüpfung zu den verschiedenen Kategorien von Informationen herzustellen, die der betroffenen Person zur Verfügung gestellt werden müssen, anstatt einen einzigen Hinweis zu verwenden.[xi] Dieser Ansatz ermöglicht es Benutzern, direkt zu dem Abschnitt der Nachricht zu navigieren, den sie lesen möchten. Bei der Erstellung einer solchen mehrfachen Benachrichtigung müssen die Verantwortlichen darauf ausgerichtet sein, einen klaren und verständlichen Überblick (oder Inhalt)

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

bereitzustellen, damit die betroffenen Personen wissen, wo sie die einzelnen Informationen finden können.

2.3.2. “Push” & “pull” Notifikationen

Die Artikel-29-Datenschutzgruppe führt auch die Verwendung von "Push" - und "Pull" -Benachrichtigungen ein. Der Hauptunterschied besteht darin, dass im letzteren Fall die Benutzer einer Seite Informationen anfordern sollen, insbesondere die Informationen über die Verarbeitung ihrer Daten, während im ersten Fall die Benachrichtigung ohne weitere Aktionen auf ihren Bildschirm "gedrängt" wird. Das WP29 enthält Beispiele für Push-Benachrichtigungen mit "Just-in-Time" -Informationshinweisen und "Pull" -Benachrichtigungen - mit Transparenz-Dashboards und "Lernt mehr"-Tutorials[xii]:

- Eine Just-in-Time-Benachrichtigung wird verwendet, um spezifische "Datenschutzinformationen" bereitzustellen, wenn sie für die betroffene Person am relevantesten sind. Dieses Format kann nützlich sein, wenn auf der Website einer lokalen Behörde nach dem Ausfüllen eines Formulars ein bestimmter Dienst online ausgeführt werden soll. Bevor der Bürger das Formular einreicht, kann eine solche Just-in-Time-Benachrichtigung erscheinen.
- Das Transparenz-Dashboard ist ein zentraler Punkt, an dem betroffene Personen "Datenschutzinformationen" einsehen und ihre Datenschutzeinstellungen verwalten können, indem sie ihre Daten auf bestimmte Arten zulassen oder verhindern.

2.3.3. Andere Arten von "geeigneten Maßnahmen"

Außerhalb der digitalen Umgebung können gemäß der Datenschutzgruppe 29 geeignete Maßnahmen sein:

- Für Papier / Papier-Umgebung: schriftliche Erklärungen, Broschüren;
- Telefonische Umgebung: mündliche Erklärungen durch eine reale Person, automatisierte oder vorab aufgezeichnete Informationen mit Optionen für detailliertere Informationen;
- QR-Codes, Sprachalarme, schriftliche Informationen auf dem Smart-Gerät, Nachrichten per SMS oder E-Mail und andere;

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

- Umgebung von Person zu Person: mündliche Erklärungen, schriftliche Erklärungen in Papierform oder Soft-Copy-Format[xiii].

2.3.4. Visualisierungen

Die DSGVO führt Visualisierungswerkzeuge ein (insbesondere Referenzierung, Symbole, Zertifizierungsmechanismen und Datenschutzsiegel und Marken). Die Idee der Icons besteht darin, die Informationen unter Verwendung standardisierter Symbole / Bilder, die in der EU anerkannt sind, den betroffenen Personen zugänglich zu machen. Die Entwicklung eines "Code of Icons" hat noch nicht begonnen. Die Datenschutz-Grundverordnung sieht auch den Einsatz von Datenschutz-Zertifizierungsmechanismen, Datenschutzsiegeln und Marken zum Nachweis der Einhaltung der Verordnung vor. Zertifizierungsmechanismen werden von den Mitgliedstaaten, den Aufsichtsbehörden, der Europäischen Datenschutzbehörde oder der Kommission eingerichtet und sollen nachweisen, dass der für die Verarbeitung Verantwortliche die DSGVO einhält und zeigt, dass er technische und organisatorische Maßnahmen zur Einhaltung der Datenschutzstandards vornimmt. Diese Formate können in Einheiten angewendet werden, die keine öffentlichen Behörden sind, wie beispielsweise eine autonome kommunale Gesellschaft.

2.4. Ausübung der Rechte von Datensubjekten

Betroffene Personen haben das Recht, von den für die Verarbeitung Verantwortlichen Daten über ihre personenbezogenen Daten zu erhalten. Die Informationen, die im Rahmen der DSGVO bereitgestellt werden müssen, sind in Art. 13 und 14 und die betroffenen Personen müssen im Gegensatz zur Ausübung ihrer sonstigen Rechte weder einen Antrag stellen noch sonstige aktive Schritte unternehmen, um sie zu erwerben (Recht auf Zugang, Berichtigung, Löschung usw.).

2.4.1. Ausnahmen von der Informationspflicht

Das Recht auf Information ist nicht absolut, d.h. es ist in bestimmten Situationen eingeschränkt.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

In bestimmten Fällen sind die lokalen Behörden von der Verpflichtung zur Bereitstellung der oben genannten Informationen befreit (gem. Art. 13 und 14). Wenn die Daten von der betroffenen Person erfasst werden, ist dies der einzige Fall, wenn sie die Information bereits besitzt (Art. 13, Abs. 4). Wenn die Daten nicht vom Subjekt erhalten werden, sind die Ausnahmen die folgenden (Art. 14, Abs. 5):

- wenn die betroffene Person bereits über die Informationen verfügt;
- wenn sich die Bereitstellung solcher Informationen als unmöglich erweist, einen unverhältnismäßigen Aufwand bedeutet oder die Erreichung der Ziele der Verarbeitung unmöglich machen oder ernsthaft beeinträchtigen würde; ein Beispiel für die Unmöglichkeit der Bereitstellung von Informationen wäre, wenn der für die Verarbeitung Verantwortliche keine Möglichkeit hat, mit der betroffenen Person Kontakt aufzunehmen;
- wenn die Beschaffung oder Offenlegung ausdrücklich durch das Recht der EU oder der Mitgliedstaaten der EU festgelegt wird, was für die lokalen Behörden die häufigste Hypothese wäre;
- wenn die personenbezogenen Daten einer beruflichen Schweigepflicht unterliegen, die durch das Recht der Union oder der Mitgliedstaaten geregelt wird, einschließlich einer gesetzlichen Verschwiegenheitspflicht; Diese Ausnahme kann für autonome kommunale Unternehmen und ähnliche Einrichtungen gelten.

Nach der WP29xiv, sollten diese Ausnahmen in der Regel eng ausgelegt und angewendet werden. Mit dieser Empfehlung sollen die Fälle begrenzt werden, in denen die für die Verarbeitung Verantwortlichen die Ausnahmen anwenden und einen besseren Schutz der Rechte der betroffenen Personen gewährleisten könnten.

3. SCHLUSSFOLGERUNG & PRAKTISCHE HINWEISE

Der Grundsatz der Transparenz ist eine der Grundlagen der DSGVO. Es bietet mehrere Garantien, dass natürliche Personen alle Informationen erhalten, die sie benötigen, um sowohl darüber informiert zu werden, welche personenbezogenen Daten über sie verarbeitet werden, als auch um ihre Rechte gemäß der Verordnung auszuüben. Die Informationen sollten leicht zugänglich sein und in klarer und verständlicher Sprache abgefasst sein.

Den lokalen Behörden wird empfohlen, eine Liste aller von der Datenschutz-Grundverordnung geforderten Informationen zu erstellen und die besten Modalitäten auszuwählen, um die Bürger zu erreichen, deren Daten sie verarbeiten. Zum Beispiel können sie

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

Informationsplakate in ihren öffentlichen Ämtern aufstellen und Flugblätter verteilen, die die Informationen unter Art.13 und Art. 14 umfassen. Elektronischen Mittel können beispielsweise nützlich sein, wenn das Unternehmen über eine Online-Site / Plattform verfügt, in bestimmten Fällen können jedoch auch Hardcopy-Formate erforderlich sein. Besondere Aufmerksamkeit sollte den Online-Diensten der lokalen Behörden gewidmet werden. Es sollte auch berücksichtigt werden, dass einige autonome kommunale Unternehmen (wie z.B. öffentliche Verkehrsunternehmen) zahlreiche Arten der Verarbeitung durchführen und mit enormen Datenbanken umgehen, daher sollten sie zusätzliche Anstrengungen unternehmen, um die Informationen unter Art. 13 und 14 richtig darzustellen.

4. EXTERNE QUELLEN & WEBLINKS

4.1. Bücher

- Voigt, P., von dem Bussche, A., The EU General Data Protection Regulation (GDPR) – A Practical Guide, Springer International Publishing (2017);
- Bird & Bird Guide to General Data Protection Regulation (2016);
- EU General Data Protection Regulation (GDPR). An Implementation and Compliance Guide, IT Governance Publishing, Cambridgeshire (2016);

4.2. Dokumente der Artikel 29 Working Party

- Article 29 Working Party, Guidelines on Data Protection Officers ('DPOs'), WP 243 rev.01;
- Article 29 Working Party, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, WP 217;

4.3. Web Links

- http://europa.eu/rapid/press-release_IP-18-386_en.htm
- https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

5. REFERENZEN

[i] The Article 29 Working Party (WP) is established on the basis of Art. 29 of Directive 95/46/EC, which will be replaced by the GDPR. The goal of the WP is to provide opinions and recommendations and to advice on personal data protection.
[ii] Article 29 Data Protection Working Party, Guidelines on transparency under Regulation 2016/679, p. 23
[iii] Ibid, p. 8
[iv] Ibid, p. 9
[v] Ibid
[vi] Ibid
[vii] Ibid, p. 21
[viii] Ibid, p. 12
[ix] Ibid, p. 15
[x] Ibid, p. 16
[xi] Ibid, p. 17
[xii] Ibid, p. 17-18
[xiii] Ibid, p. 18-19
[xiv] Ibid, p. 25

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

ProLegis

OFFENLEGUNG VON INFORMATIONEN ODER AUSKUNFTSRECHT DER BE-TROFFENEN PERSON

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

Dissemination Level:		
PU	Public	
CO	Confidential, only for members of the consortium (including the Commission Services)	
EU-RES	Classified Information: RESTREINT UE (Commission Decision 2005/444/EC)	
EU-CON	Classified Information: CONFIDENTIEL UE (Commission Decision 2005/444/EC)	
EU-SEC	Classified Information: SECRET UE (Commission Decision 2005/444/EC)	
Document version control:		
Version	**Author(s)**	**Date**
Version 1	Developed by:	
Version 1	Reviewed & updated by:	
Version 2	Translated by: VICESSE	21/06/18

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

Inhaltsverzeichnis

1. RECHTLICHER RAHMEN 4
1.1. DSGVO 4
2. GRUNDLAGEN 6
3.1. Offenlegung 7
3.2. Wie viel Zeit hat der Controller zu beantworten (Deadline)? 8
3.3. In welcher Form kann Anspruch erhoben werden und wie soll diese beantwortet werden? 9
3.4. Hat die Identität des Antragstellers die zu prüfende Datensubstanz? 9
3.5. Kosten? Möge die Information erstattet werden? 10
3.6. Ist der Antragsteller verpflichtet, sich an der Offenlegung zu beteiligen? 10
3.7. Müssen die Rechte Dritter bei der Bereitstellung von Informationen berücksichtigt werden? 11
4. CHECKLISTE FÜR DIE OFFENLEGUNG VON INFORMATIONEN AUF ANFRAGE 11
4.1. Muss ich Auskunft geben? 11
4.2. Identitätsprüfung 11
4.3. Gibt es eine übermäßige oder offensichtlich unbegründete Bewerbung? 12
4.4. Werden personenbezogene Daten des Antragstellers überhaupt verarbeitet? 12
4.5. Welche Daten und Informationen muss der Controller bereitstellen? 12
4.6. Ausgabe der Informationen 13
5. Externe Quellen & Weblinks 14
5.1. Bücher und Artikel 14
5.2. Andere Dokumente und Fälle 14

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

1. RECHTLICHER RAHMEN

1.1. DSGVO

Artikel 15

Auskunftsrecht der betroffenen Person

(1) Die betroffene Person hat das Recht, von dem Verantwortlichen eine Bestätigung darüber zu verlangen, ob sie betreffende personenbezogene Daten verarbeitet werden; ist dies der Fall, so hat sie ein Recht auf Auskunft über diese personenbezogenen Daten und auf folgende Informationen:

a) die Verarbeitungszwecke;

b) die Kategorien personenbezogener Daten, die verarbeitet werden;

c) die Empfänger oder Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, insbesondere bei Empfängern in Drittländern oder bei internationalen Organisationen;

d) falls möglich die geplante Dauer, für die die personenbezogenen Daten gespeichert werden, oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer;

e) das Bestehen eines Rechts auf Berichtigung oder Löschung der sie betreffenden personenbezogenen Daten oder auf Einschränkung der Verarbeitung durch den Verantwortlichen oder eines Widerspruchsrechts gegen diese Verarbeitung;

f) das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde;

g) wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben werden, alle verfügbaren Informationen über die Herkunft der Daten;

h) das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling gemäß Artikel 22 Absätze 1 und 4 und — zumindest in diesen Fällen — aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person.

(2) Werden personenbezogene Daten an ein Drittland oder an eine internationale Organisation übermittelt, so hat die betroffene Person das Recht, über die geeigneten Garantien gemäß Artikel 46 im Zusammenhang mit der Übermittlung unterrichtet zu werden.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

(3) Der Verantwortliche stellt eine Kopie der personenbezogenen Daten, die Gegenstand der Verarbeitung sind, zur Verfügung. Für alle weiteren Kopien, die die betroffene Person beantragt, kann der Verantwortliche ein angemessenes Entgelt auf der Grundlage der Verwaltungskosten verlangen. Stellt die betroffene Person den Antrag elektronisch, so sind die Informationen in einem gängigen elektronischen Format zur Verfügung zu stellen, sofern sie nichts anderes angibt.

(4) Das Recht auf Erhalt einer Kopie gemäß Absatz 1b darf die Rechte und Freiheiten anderer Personen nicht beeinträchtigen.

Erwägungsgründe:

(63) Eine betroffene Person sollte ein Auskunftsrecht hinsichtlich der sie betreffenden personenbezogenen Daten, die erhoben worden sind, besitzen und dieses Recht problemlos und in angemessenen Abständen wahrnehmen können, um sich der Verarbeitung bewusst zu sein und deren Rechtmäßigkeit überprüfen zu können. Dies schließt das Recht betroffene Personen auf Auskunft über ihre eigenen gesundheitsbezogenen Daten ein, etwa Daten in ihren Patientenakten, die Informationen wie beispielsweise Diagnosen, Untersuchungsergebnisse, Befunde der behandelnden Ärzte und Angaben zu Behandlungen oder Eingriffen enthalten. Jede betroffene Person sollte daher ein Anrecht darauf haben zu wissen und zu erfahren, insbesondere zu welchen Zwecken die personenbezogenen Daten verarbeitet werden und, wenn möglich, wie lange sie gespeichert werden, wer die Empfänger der personenbezogenen Daten sind, nach welcher Logik die automatische Verarbeitung personenbezogener Daten erfolgt und welche Folgen eine solche Verarbeitung haben kann, zumindest in Fällen, in denen die Verarbeitung auf Profiling beruht. Nach Möglichkeit sollte der Verantwortliche den Fernzugang zu einem sicheren System bereitstellen können, der der betroffenen Person direkten Zugang zu ihren personenbezogenen Daten ermöglichen würde. Dieses Recht sollte die Rechte und Freiheiten anderer Personen, etwa Geschäftsgeheimnisse oder Rechte des geistigen Eigentums und insbesondere das Urheberrecht an Software, nicht beeinträchtigen. Dies darf jedoch nicht dazu führen, dass der betroffenen Person jegliche Auskunft verweigert wird. Verarbeitet der Verantwortliche eine große Menge von Informationen über die betroffene Person, so sollte er verlangen können, dass die betroffene Person präzisiert, auf welche Information oder welche Verarbeitungsvorgänge sich ihr Auskunftsersuchen bezieht, bevor er ihr Auskunft erteilt.

(64) Der Verantwortliche sollte alle vertretbaren Mittel nutzen, um die Identität einer Auskunft suchenden betroffenen Person zu überprüfen, insbesondere im Rahmen von

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

Online-Diensten und im Fall von Online-Kennungen. Ein Verantwortlicher sollte personenbezogene Daten nicht allein zu dem Zweck speichern, auf mögliche Auskunftsersuchen reagieren zu können.

2. GRUNDLAGEN

Die Datenschutz-Grundverordnung enthält in Artikel 15 das Recht, alle Informationen über die betroffene Person durch den Conroller (z.B. Firma, Arbeitgeber, Krankenhausbetreiber gegenüber dieser betroffenen Person auf Anfrage offenzulegen (z.B. Kunde, Arbeitnehmer, Bewerber, Patient, im Folgenden "betroffene Person")). Dies wird als "Zugriffsrecht der betroffenen Person (auf ihre Daten)" bezeichnet. Der Zweck dieses Rechts besteht darin, dass der Betroffene Informationen über den Inhalt und die Einzelheiten der über ihn verarbeiteten Daten erhalten kann, um gegebenenfalls weitere Rechte des Betroffenen geltend zu machen (z. B. eine Berichtigung oder Löschung nach Art. 16 DSGVO)) oder die Rechtmäßigkeit der Verarbeitung.

Dieses Recht ist eine zentrale Institution des Datenschutzrechts, da es oft als Grundlage für die Ausübung anderer Rechte durch die betroffene Person betrachtet werden muss. Obwohl Datenschutzbehörden nach der DSGVO befugt sind, einen für die Verarbeitung Verantwortlichen ohne besondere Beschwerde zu auditieren, ist es in der Praxis (aufgrund begrenzter Ressourcen von Datenschutzbehörden) typischerweise eine unvollständige oder verspätete Offenlegung gemäß dem Zugriffsrecht der betroffenen Personen, das die Datenschutzbehörde auf den Plan ruft. Daher sollten Controller für diesen Prozess gut vorbereitet sein.

Die beste Vorbereitung sind jedoch gut strukturierte und bestmögliche detaillierte Aufzeichnungen der Verarbeitungsaktivitäten. Je besser diese Dokumentation entlang der Geschäftsprozesse gestaltet ist, für die personenbezogene Daten verarbeitet werden, desto leichter ist es, die jeweiligen Daten eines bestimmten Themas innerhalb der Anwendungen auch rechtzeitig zu finden.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

3. EINZELHEITEN DER WEITERGABE VON INFORMATIONEN AN DIE BETROFFENE PERSON

3.1. Offenlegung

Das Zugriffsrecht enthält drei Ansprüche für die betroffene Person:

i. Das Recht, den für die Verarbeitung Verantwortlichen zu fragen, ob personenbezogene Daten des anfragenden Subjekts verarbeitet werden oder nicht; eine Anfrage sollte daher auch "negativ" beantwortet werden, wenn keine Daten über diese Person verarbeitet werden (sog. "negative Information"): "Wir verarbeiten keine Daten über Sie.");

ii. Das Recht, eine Kopie der personenbezogenen Daten zu erhalten, die Gegenstand der Verarbeitung sind (für zusätzliche Kopien, die von der betroffenen Person angefordert werden, kann der für die Verarbeitung Verantwortliche eine angemessene Gebühr auf der Grundlage der Verwaltungskosten erheben.) Wenn der Betroffene den Antrag elektronisch einreicht, sofern nichts anderes angegeben ist, werden die Informationen in einem gemeinsamen elektronischen Format bereitgestellt.

iii. Das Recht, folgende Informationen zu erhalten:

Art 15 Abs 1 GDPR	
lit a	der Zweck der Verarbeitung
lit b	**Kategorien von verarbeiteten persönlichen Daten**
lit c	die Empfänger oder Kategorien von Empfängern, denen die personenbezogenen Daten mitgeteilt wurden oder werden, insbesondere Empfänger in Drittländern oder internationale Organisationen
lit d	soweit möglich, den vorgesehenen Zeitraum, in dem die personenbezogenen Daten gespeichert werden, oder, wenn dies nicht möglich ist, die Kriterien, die für die Festlegung dieser Frist verwendet wurden;
lit e	das Recht, von dem für die Verarbeitung Verantwortlichen die Berichtigung oder Löschung personenbezogener Daten oder die Einschränkung der Verarbeitung personenbezogener Daten in Bezug auf die betroffene Person zu verlangen oder einer solchen Verarbeitung zu widersprechen;
lit f	das Recht, eine Beschwerde bei einer Aufsichtsbehörde einzureichen;

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

lit g	wenn die personenbezogenen Daten nicht von der betroffenen Person erhoben werden, alle verfügbaren Informationen zu ihrer Quelle;
lit h	das Vorhandensein einer automatisierten Entscheidungsfindung, einschließlich Profilerstellung, gemäß Artikel 22 Absätze 1 und 4 und zumindest in diesen Fällen eine aussagekräftige Information über die betreffende Logik sowie die Bedeutung und die beabsichtigten Folgen einer solchen Verarbeitung für die betroffene Person.
Abs 2	Werden personenbezogene Daten an ein Drittland oder an eine internationale Organisation übermittelt, so hat die betroffene Person das Recht, über die geeigneten Garantien gemäß Artikel 46 in Bezug auf die Übermittlung informiert zu werden.

Hinweis: Gemäß Artikel 23, u.a. das Recht auf Information ist durch separate Rechtsvorschriften eingeschränkt.

3.2. Wie viel Zeit hat der Controller zu beantworten (Deadline)?

Grundsätzlich muss das Auskunftsersuchen unverzüglich, spätestens jedoch innerhalb eines Monats nach Eingang des Antrags beantwortet werden (Art. 12 Abs. 3 DSGVO). Dieser Zeitraum kann erforderlichenfalls um weitere zwei Monate verlängert werden, wobei die Komplexität und die Anzahl der Anträge zu berücksichtigen sind. Der für die Verarbeitung Verantwortliche informiert die betroffene Person innerhalb von einem Monat nach Erhalt des Antrags über die Verlängerung der Frist, zusammen mit den Gründen für die Verzögerung. Wenn die betroffene Person den Antrag elektronisch einreicht, wird die betroffene Person, sofern nicht anders angegeben, wenn möglich, auf elektronischem Wege informiert.

Trifft der für die Verarbeitung Verantwortliche das Ersuchen der betroffenen Person nicht, so hat er die betroffene Person unverzüglich, spätestens jedoch einen Monat nach Eingang des Ersuchens, über die Gründe dafür und über die Möglichkeit der Einreichung einer Beschwerde bei einer Aufsichtsbehörde oder bei der Aufsichtsbehörde zu informieren einen Rechtsbehelf einlegen.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

3.3. In welcher Form kann Anspruch erhoben werden und wie soll diese beantwortet werden?

Es besteht kein Formzwang, das Auskunftsersuchen kann mündlich, schriftlich oder in digitaler Form (z.B. per E-Mail) gestellt werden. Die Antwort auf ein Auskunftsersuchen kann in jeder geeigneten Form erfolgen, wobei Folgendes zu beachten ist:

- ✓ Eine schriftliche Anfrage wird am besten schriftlich beantwortet. Eine gängige Methode war in der Vergangenheit, dass der Antragsgegner eine Kopie eines Ausweisdokuments (amtlicher Ausweis) zu seinem Antrag eingereicht hat und der Verantwortliche die Antwort als Einschreiben (ohne Zusteller) gegeben hat.
- ✓ Auf Wunsch des Antragstellers können die Informationen mündlich übermittelt werden, sofern die Identität der betroffenen Person in einer anderen Form festgestellt wurde.
- ✓ Wenn die betroffene Person den Antrag elektronisch einreicht (z. B. per E-Mail), müssen die Informationen in einem gemeinsamen elektronischen Format bereitgestellt werden, sofern nichts anderes angegeben ist. Wenn möglich, kann der Controller auch einen Fernzugriff auf ein sicheres System bereitstellen, das der betroffenen Person direkten Zugriff auf ihre persönlichen Informationen gibt.

Achtung! Alle Mitteilungen müssen in einer klaren und einfachen Sprache in einer präzisen, transparenten, verständlichen und leicht zugänglichen Form übermittelt werden (dies gilt insbesondere für Informationen, die sich speziell an Kinder richten). Wie in der Vergangenheit müssen die in der Antwort enthaltenen Abkürzungen vom Controller in seiner Antwort erläutert werden.

3.4. Hat die Identität des Antragstellers die zu prüfende Datensubstanz?

Ja. Die Identität der Person, die die Information beantragt (die betreffende Person), muss klar sein, da der für die Verarbeitung Verantwortliche zusätzliche Informationen anfordern kann, wenn er "begründete Zweifel" über die Identität der natürlichen Person hat (siehe Art. 12 Abs. 6).[1]

[1] See also Souhrada-Kirchmayer, The right of access to the DSGVO, in Jahnel [Hrsg], Yearbook 17. Data Protection Law [2017] 86 f.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

Nach Erwägungsgrund 64 sollte der für die Verarbeitung Verantwortliche alle angemessenen Mittel einsetzen, um die Identität der betroffenen Person zu überprüfen, insbesondere im Zusammenhang mit Online-Diensten und im Fall von Online-Identifikatoren.

Die Identitätsauthentifizierung sollte so gestaltet sein, dass die Verpflichtung zur Gewährleistung der Datensicherheit im Einklang mit dem Risiko erfüllt wird, da andernfalls eine Datenverletzung auftreten könnte, wenn die Daten an den falschen Empfänger übermittelt werden.

In Österreich war es nach dem früheren Datenschutzgesetz (DSG 2000) üblich, dass der Antragsteller eine Kopie eines Ausweises (amtlicher Ausweis) zu seiner Bewerbung einreichte und der Verantwortliche der Post die Antwort als "persönlichen" Einschreiben gab. Die Identität kann jedoch auch aus der Situation klar sein, z.B. wenn es einen ständigen Kontakt mit dem Informationsanbieter gibt und dieser (und seine Adresse) daher bekannt ist[2].

3.5. Kosten? Möge die Information erstattet werden?

Grundsätzlich müssen die Informationen kostenlos zur Verfügung gestellt werden (siehe Art. 12 Abs. 5 DSGVO). Im Falle offensichtlich unbegründeter oder insbesondere häufiger Wiederholungen übermäßiger Anfragen einer betroffenen Person kann der für die Verarbeitung Verantwortliche jedoch entweder

a) eine angemessene Gebühr unter Berücksichtigung der Verwaltungskosten für die Notifizierung, die Übermittlung oder die Durchführung der beantragten Maßnahme verlangen; oder

b) sich weigern, auf den Antrag zu reagieren.

3.6. Ist der Antragsteller verpflichtet, sich an der Offenlegung zu beteiligen?

Ja, selbst wenn eine Mitwirkungspflicht nur in Erwägungsgrund 63 erwähnt wird, wird in der bisher veröffentlichten Literatur im Wesentlichen davon ausgegangen, dass sie existiert (das wurde auch in Österreich unter DSG 2000 anerkannt): "Wenn der für die Verarbeitung Verantwortliche eine große Menge an Daten des Betroffenen verarbeitet, sollte der für die Verarbeitung Verantwortliche in der Lage sein zu verlangen, dass der

[2] See e.g. the jurisprudence of the Austrian High Courts: VwGH 4.7.2016, Ra 2016/04/0014; OGH 25.2.1993, 6 Ob 6/93)

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

Betroffene vor der Übermittlung der Informationen die Informationen oder Verarbeitungstätigkeiten angibt, auf die sich der Antrag bezieht. "[3]

3.7. Müssen die Rechte Dritter bei der Bereitstellung von Informationen berücksichtigt werden?

Ja, siehe insbesondere Artikel 15 (4) DSGVO, wonach das Recht auf Erhalt einer Kopie die Rechte und Freiheiten anderer nicht beeinträchtigen darf. Siehe auch Erwägungsgrund 63: "Dieses Recht sollte die Rechte oder Freiheiten anderer, einschließlich Geschäftsgeheimnisse oder geistiges Eigentum und insbesondere das Urheberrecht zum Schutz der Software, nicht beeinträchtigen. Das Ergebnis dieser Erwägungen sollte jedoch nicht die Weigerung sein, alle Informationen bereitzustellen an die betroffene Person. "

Es ist daher notwendig, die zu veröffentlichenden Daten zu kontrollieren, in der Regel müssen personenbezogene Daten Dritter (zum Beispiel der Name der Person, die den Kunden behandelt und in der Kundendatei aufgeführt ist) aus der Datenkopie gelöscht werden.

4. CHECKLISTE FÜR DIE OFFENLEGUNG VON INFORMATIONEN AUF ANFRAGE

4.1. Muss ich Auskunft geben?

Wenn beispielsweise eine Organisation lediglich ein Bearbeiter ist, aber dennoch eine Anfrage erhält, muss sie diese sofort an die zuständige Person weiterleiten.

4.2. Identitätsprüfung

Siehe obige Frage. 5. Wenn Zweifel an der Identität bestehen: Fordern Sie einen Nachweis an!

[3] recital 63.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

4.3. Gibt es eine übermäßige oder offensichtlich unbegründete Bewerbung?

Z.B. der Antragsteller erhielt oft die gleichen Informationen, möglicherweise Kostenbeteiligung.

4.4. Werden personenbezogene Daten des Antragstellers überhaupt verarbeitet?

Sind keine Daten über den Antragsteller gespeichert oder wurden die Daten bereits gelöscht oder wurden die Daten irreversibel anonymisiert, werden keine personenbezogenen Daten verarbeitet und es wird eine sogenannte negative Information übermittelt ("Wir verarbeiten keine Daten über Sie ").

4.5. Welche Daten und Informationen muss der Controller bereitstellen?

Siehe auch oben Kapitel 2.

Alle Daten müssen zur Verfügung gestellt werden, die von der betroffenen Person gespeichert werden. Je nach Komplexität der Systeme muss im Vorfeld (hinsichtlich des Verarbeitungsverzeichnisses) berücksichtigt werden, in welchen Systemen Daten zu welcher Kategorie betroffener Personen gefunden werden können. Darüber hinaus müssen die in Artikel 15 Absatz 1 DSGVO aufgeführten Informationen bereitgestellt werden. Rechte Dritter sind zu beachten (insbes. Geschäftsgeheimnisse und Daten Dritter sind zu streichen / geschwärzt), siehe Punkt 8.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

4.6. Ausgabe der Informationen

Beispiel für eine Offenlegung von Informationen gemäß Artikel 15 DSGVO

Ihre Anfrage nach Informationen

Sehr geehrte Damen und Herren [Name],

1. Ihre Bewerbung von [Datum] zu Informationen gemäß Art. 15 DSVO, die wir am [Datum] erhalten haben, können wie folgt beantwortet werden:

2. [Im Falle einer Antwort innerhalb eines Monats nach Erhalt] Wir bestätigen hiermit rechtzeitig, dass wir personenbezogene Daten über Sie verarbeiten.

[im Falle der Verlängerung gemäß der Kunst. 12 (3) DSGVO] Wie in dem Schreiben vom [Datum] angegeben, haben wir die Gelegenheit genutzt, die Frist aufgrund der Komplexität des Antrags oder der Anzahl Ihrer Anträge auf drei Monate zu verlängern, weitere Erläuterungen sind erforderlich].

3. [wenn keine Daten verarbeitet werden] Keine persönlichen Daten werden verarbeitet. [Dann weiter mit Textbaustein Nr. 9].

[Wenn Daten verarbeitet werden] Speziell verarbeiten wir die folgenden Daten über Sie: [hier ist eine Liste der tatsächlich zu verarbeitenden Daten].

Ausdrucke / Kopien aus der relevanten Datenverarbeitung finden Sie im Anhang. Jede Schwärzung oder Unterlassung wurde vorgenommen, um die Rechte und Freiheiten anderer nicht zu beeinträchtigen oder weil die Informationen Sie oder Ihre persönlichen Informationen nicht betreffen.

4. [wenn keine Daten von der betroffenen Person erhoben wurden]: Wir haben Ihre Daten von [verfügbaren Informationen zur Herkunft Ihrer Daten, z. B. Firma XY] erhalten.

5. [falls anwendbar] Wir werden automatisierte Entscheidungsfindung / Profiling-Verfahren verwenden, die eine rechtliche Wirkung auf Sie haben oder in ähnlicher Weise auf Sie wirken: [Bitte füllen Sie aussagekräftige Informationen über die involvierte Logik und die Implikationen und Implikationen aus].

6. Sie haben das Recht auf Berichtigung, Löschung, Einschränkung und das Recht, die Verarbeitung Ihrer personenbezogenen Daten zu widerrufen. Kontaktieren Sie uns dazu. Wenn Sie der Ansicht sind, dass die Verarbeitung Ihrer Daten gegen das Datenschutzgesetz verstößt oder Ihre Datenschutzansprüche in anderer Weise verletzt wurden, können Sie sich bei der Aufsichtsbehörde beschweren. In Österreich ist die Datenschutzbehörde zuständig.

Mit freundlichen Grüßen

….

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

5. Externe Quellen & Weblinks

5.1. Bücher und Artikel

- Souhrada-Kirchmayer, The right of access to the DSGVO, in Jahnel [Hrsg], Yearbook 17. Data Protection Law [2017] 86 f.
- Martini in Paal/Pauly (Ed.), Datenschutz-Grundverordnung (2016)

5.2. Andere Dokumente und Fälle

- Jurisprudence of the Austrian High Courts: VwGH 4.7.2016, Ra 2016/04/0014; OGH 25.2.1993, 6 Ob 6/93)Web Links
- To compare the changes to directive 95/46/EC see https://gdpr.report/news/2017/11/20/gdpr-subject-access-requests/

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

ProLegis

ΝΟΜΙΚΟΙ ΛΟΓΟΙ ΓΙΑ ΤΗΝ ΕΠΕΞΕΡΓΑΣΙΑ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

ProLegis

Contents

1. LEGAL FRAMEWORK 4
   1.1. Charter of Fundamental Rights of EU 4
   1.2. GDPR 4
2. LEGAL GROUNDS FOR PERSONAL DATA PROCESSING UNDER GDPR 12
   2.1. Consent 12
      2.1.1. Meaning & legal requirements 12
      2.1.2. Applicability in the context of the Local authorities' activity 14
   2.2. Performance/ conclusion of contract with the data subject 16
      2.2.1. Meaning & legal requirements 16
      2.2.2. Applicability in the context of the Local authorities' activity 17
   2.3. Legal obligation 17
      2.3.1. Meaning & legal requirements 17
      2.3.2. Applicability in the context of the Local authorities' activity 18
   2.4. Vital interest 19
      2.4.1. Meaning & legal requirements 19
      2.4.2. Applicability in the context of the Local authorities' activity 19
   2.5. Task carried out in the public interest/ exercise of official authority 20
      2.5.1. Meaning & legal requirements 20
      2.5.2. Applicability in the context of the Local authorities' activity 21
   2.6. Legitimate Interests 21
      2.6.1. Meaning & legal requirements 21
      2.6.2. Applicability in the context of the Local authorities' activity 22
3. CONCLUSION & PRACTICAL ADVICES 23

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

4. EXTERNAL SOURCES & WEBLINKS 23

Books 23

Documents of the Article 29 Working Party 23

Web Links 24

5. REFERENCES 24

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

1. ΝΟΜΙΚΟ ΠΛΑΙΣΙΟ

1.1. Χάρτης Θεμελιωδών Δικαιωμάτων της ΕΕ

Άρθρο 8

Προστασία των δεδομένων προσωπικού χαρακτήρα

1. Κάθε πρόσωπο έχει δικαίωμα στην προστασία των δεδομένων προσωπικού χαρακτήρα που το αφορούν.

2. Η επεξεργασία αυτών των δεδομένων πρέπει να γίνεται νομίμως, για καθορισμένους σκοπούς και ***με βάση τη συγκατάθεση του ενδιαφερομένου ή για άλλους θεμιτούς λόγους που προβλέπονται από το νόμο.*** *Κάθε πρόσωπο δικαιούται να έχει πρόσβαση στα συλλεγέντα δεδομένα που το αφορούν και να επιτυγχάνει τη διόρθωσή τους.*

3. Ο σεβασμός των κανόνων αυτών υπόκειται στον έλεγχο ανεξάρτητης αρχής.

1.2. ΓΚΠΔ (Γενικός κανονισμός για την προστασία των δεδομένων)

Αιτιολογική σκέψη (42)

[...]Για να θεωρηθεί η συγκατάθεση εν επιγνώσει, το υποκείμενο των δεδομένων θα πρέπει να γνωρίζει τουλάχιστον την ταυτότητα του υπευθύνου επεξεργασίας και τους σκοπούς της επεξεργασίας για την οποία προορίζονται τα δεδομένα προσωπικού χαρακτήρα. Η συγκατάθεση δεν θα πρέπει να θεωρείται ότι δόθηκε ελεύθερα αν το υποκείμενο των δεδομένων δεν έχει αληθινή ή ελεύθερη επιλογή ή δεν είναι σε θέση να αρνηθεί ή να αποσύρει τη συγκατάθεσή του χωρίς να ζημιωθεί.

Αιτιολογική σκέψη (43)

Για να διασφαλιστεί ότι η συγκατάθεση έχει δοθεί ελεύθερα, η συγκατάθεση δεν θα πρέπει να παρέχει έγκυρη νομική βάση για την επεξεργασία δεδομένων προσωπικού χαρακτήρα σε μια συγκεκριμένη περίπτωση, όταν υπάρχει σαφής ανισότητα μεταξύ του υποκειμένου των δεδομένων και του υπευθύνου επεξεργασίας, ***ιδίως στις περιπτώσεις που ο υπεύθυνος επεξεργασίας είναι δημόσια αρχή*** *και είναι επομένως σχεδόν απίθανο να έχει δοθεί η συγκατάθεση ελεύθερα σε όλες τις περιστάσεις αυτής της ειδικής κατάστασης. Η συγκατάθεση θεωρείται ότι δεν έχει παρασχεθεί ελεύθερα, εάν δεν επιτρέπεται να δοθεί χωριστή συγκατάθεση σε διαφορετικές πράξεις επεξεργασίας δεδομένων προσωπικού χαρακτήρα, ακόμη και αν*

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

ενδείκνυται στη συγκεκριμένη περίπτωση, ή όταν η εκτέλεση μιας σύμβασης, συμπεριλαμβανομένης της παροχής μιας υπηρεσίας, προϋποθέτει τη συγκατάθεση, ακόμη και αν η συγκατάθεση αυτή δεν είναι αναγκαία για την εν λόγω εκτέλεση.

Αιτιολογική σκέψη (44)

*Η επεξεργασία θα πρέπει επίσης να είναι σύννομη εφόσον **είναι αναγκαία στο πλαίσιο σύμβασης ή πρόθεσης σύναψης σύμβασης**.*

Αιτιολογική σκέψη (45)

*Όταν η επεξεργασία διενεργείται σύμφωνα με **νομική υποχρέωση** την οποία υπέχει ο υπεύθυνος επεξεργασίας ή όταν είναι αναγκαία για την εκπλήρωση καθήκοντος που εκτελείται προς το δημόσιο συμφέρον ή κατά την άσκηση δημόσιας εξουσίας, η επεξεργασία θα πρέπει να έχει βάση στο δίκαιο της Ένωσης ή κράτους μέλους. Ο παρών κανονισμός δεν απαιτεί συγκεκριμένο νόμο για κάθε μεμονωμένη επεξεργασία. Μπορεί να αρκεί ένας μόνο νόμος ως βάση για περισσότερες από μία πράξεις επεξεργασίας με βάση νομική υποχρέωση στην οποία υπόκειται ο υπεύθυνος επεξεργασίας ή εάν η επεξεργασία είναι αναγκαία για την εκπλήρωση καθήκοντος που εκτελείται προς το δημόσιο συμφέρον ή κατά την άσκηση δημόσιας εξουσίας. Επίσης, ο καθορισμός του σκοπού της επεξεργασίας θα πρέπει να εναπόκειται στο δίκαιο της Ένωσης ή κράτους μέλους. Επιπλέον, το εν λόγω δίκαιο θα μπορούσε να προσδιορίζει τις γενικές προϋποθέσεις του παρόντος κανονισμού που διέπουν τη σύννομη επεξεργασία δεδομένων προσωπικού χαρακτήρα και να θεσπίζει προδιαγραφές για τον καθορισμό του υπευθύνου επεξεργασίας, του είδους των δεδομένων προσωπικού χαρακτήρα που υπόκεινται σε επεξεργασία, των εκάστοτε υποκειμένων των δεδομένων, των οντοτήτων στις οποίες μπορούν να κοινολογούνται τα δεδομένα προσωπικού χαρακτήρα, των περιορισμών σκοπού, της περιόδου αποθήκευσης και άλλων μέτρων για την εξασφάλιση σύννομης και δίκαιης επεξεργασίας. Επίσης, θα πρέπει να εναπόκειται στο ενωσιακό δίκαιο ή στο δίκαιο των κρατών μελών ο καθορισμός του κατά πόσον ο υπεύθυνος επεξεργασίας που εκπληρώνει καθήκον που εκτελείται προς το δημόσιο συμφέρον ή κατά την άσκηση δημόσιας εξουσίας θα πρέπει να είναι δημόσια αρχή ή άλλο φυσικό ή νομικό πρόσωπο που διέπεται από το δημόσιο δίκαιο ή, σε περίπτωση που αυτό δικαιολογείται από λόγους δημόσιου συμφέροντος, μεταξύ άλλων για λόγους υγείας, όπως η δημόσια υγεία και η κοινωνική προστασία και η διαχείριση των υπηρεσιών υγειονομικής περίθαλψης, από το ιδιωτικό δίκαιο, όπως μία επαγγελματική οργάνωση.*

Αιτιολογική σκέψη (46)

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

Η επεξεργασία δεδομένων προσωπικού χαρακτήρα θα πρέπει επίσης να θεωρείται σύννομη όταν είναι αναγκαία για την προστασία ***συμφέροντος που είναι ουσιώδες για τη ζωή του υποκειμένου των δεδομένων ή άλλου φυσικού προσώπου.*** *Η επεξεργασία δεδομένων προσωπικού χαρακτήρα με βάση το ζωτικό συμφέρον άλλου φυσικού προσώπου θα πρέπει κατ' αρχήν να διενεργείται μόνο εάν είναι πρόδηλο ότι η επεξεργασία δεν μπορεί να έχει άλλη νομική βάση. Ορισμένοι τύποι επεξεργασίας μπορούν να χρησιμεύσουν αφενός για σημαντικούς λόγους δημόσιου συμφέροντος και αφετέρου για τα ζωτικά συμφέροντα του υποκειμένου των δεδομένων, όπως, για παράδειγμα, όταν η επεξεργασία είναι απαραίτητη για ανθρωπιστικούς σκοπούς, μεταξύ άλλων για την παρακολούθηση επιδημιών και της εξάπλωσής τους ή σε καταστάσεις επείγουσας ανθρωπιστικής ανάγκης, ιδίως δε σε περιπτώσεις φυσικών και ανθρωπογενών καταστροφών.*

Αιτιολογική σκέψη (47)

Τα ***έννομα συμφέροντα του υπευθύνου επεξεργασίας, περιλαμβανομένων εκείνων ενός υπευθύνου επεξεργασίας στον οποίο μπορούν να κοινολογηθούν τα δεδομένα προσωπικού χαρακτήρα ή τρίτων****, μπορεί να παρέχουν τη νομική βάση για την επεξεργασία, υπό τον όρο ότι δεν υπερισχύουν των συμφερόντων ή των θεμελιωδών δικαιωμάτων και ελευθεριών του υποκειμένου των δεδομένων, λαμβάνοντας υπόψη τις θεμιτές προσδοκίες των υποκειμένων των δεδομένων βάσει της σχέσης τους με τον υπεύθυνο επεξεργασίας. Τέτοιο έννομο συμφέρον θα μπορούσε λόγου χάρη να υπάρχει όταν υφίσταται σχετική και κατάλληλη σχέση μεταξύ του υποκειμένου των δεδομένων και του υπευθύνου επεξεργασίας, όπως αν το υποκείμενο των δεδομένων είναι πελάτης του υπευθύνου επεξεργασίας ή βρίσκεται στην υπηρεσία του. Εν πάση περιπτώσει η ύπαρξη έννομου συμφέροντος θα χρειαζόταν προσεκτική αξιολόγηση, μεταξύ άλλων ως προς το κατά πόσον το υποκείμενο των δεδομένων, κατά τη χρονική στιγμή και στο πλαίσιο της συλλογής των δεδομένων προσωπικού χαρακτήρα, μπορεί εύλογα να αναμένει ότι για τον σκοπό αυτό μπορεί να πραγματοποιηθεί επεξεργασία. Ειδικότερα, τα συμφέροντα και τα θεμελιώδη δικαιώματα του υποκειμένου των δεδομένων θα μπορούσαν να υπερισχύουν των συμφερόντων του υπευθύνου επεξεργασίας, όταν τα δεδομένα προσωπικού χαρακτήρα υποβάλλονται σε επεξεργασία σε περιπτώσεις κατά τις οποίες το υποκείμενο των δεδομένων δεν αναμένει ευλόγως περαιτέρω επεξεργασία των δεδομένων του. Δεδομένου ότι εναπόκειται στον νομοθέτη να παρέχει διά νόμου τη νομική βάση για την επεξεργασία δεδομένων προσωπικού χαρακτήρα από τις δημόσιες αρχές, η εν λόγω νομική βάση δεν θα πρέπει να εφαρμόζεται στην επεξεργασία από τις δημόσιες αρχές κατά την εκπλήρωση των καθηκόντων τους. Η επεξεργασία δεδομένων προσωπικού χαρακτήρα, στον βαθμό που είναι αυστηρά*

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

αναγκαία για τους σκοπούς πρόληψης της απάτης, συνιστά επίσης έννομο συμφέρον του ενδιαφερόμενου υπευθύνου επεξεργασίας. Η επεξεργασία δεδομένων προσωπικού χαρακτήρα για σκοπούς άμεσης εμπορικής προώθησης μπορεί να θεωρηθεί ότι διενεργείται χάριν έννομου συμφέροντος.

Αιτιολογική σκέψη (48)

Οι υπεύθυνοι επεξεργασίας που είναι μέλη ομίλου επιχειρήσεων ή ιδρυμάτων που συνδέονται με κεντρικό φορέα ενδέχεται να έχουν έννομο συμφέρον να διαβιβάζουν δεδομένα προσωπικού χαρακτήρα εντός του ομίλου επιχειρήσεων για εσωτερικούς διοικητικούς σκοπούς, συμπεριλαμβανομένης της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα πελατών ή εργαζομένων. Οι γενικές αρχές της διαβίβασης δεδομένων προσωπικού χαρακτήρα, εντός ομίλου επιχειρήσεων, προς επιχείρηση εγκατεστημένη σε τρίτη χώρα δεν θίγονται.

Αιτιολογική σκέψη (49)

Η επεξεργασία δεδομένων προσωπικού χαρακτήρα, στον βαθμό που είναι αυστηρά αναγκαία και ανάλογη για τους σκοπούς της διασφάλισης της ασφάλειας δικτύων και πληροφοριών, δηλαδή της ικανότητας ενός δικτύου ή ενός συστήματος πληροφοριών να ανθίσταται, σε ένα δεδομένο επίπεδο εμπιστοσύνης, σε τυχαία γεγονότα ή παράνομες ή κακόβουλες ενέργειες οι οποίες θέτουν σε κίνδυνο τη διαθεσιμότητα, τη γνησιότητα, την ακεραιότητα και την εμπιστευτικότητα αποθηκευμένων ή διαβιβαζόμενων δεδομένων προσωπικού χαρακτήρα, καθώς και της ασφάλειας των σχετικών υπηρεσιών που προσφέρουν τα εν λόγω δίκτυα και συστήματα ή που είναι προσπελάσιμες μέσω των εν λόγω δικτύων και συστημάτων, ή που προσφέρονται από δημόσιες αρχές, από ομάδες αντιμετώπισης έκτακτων αναγκών στην πληροφορική (CERT), από ομάδες παρέμβασης για συμβάντα που αφορούν την ασφάλεια των υπολογιστών (CSIRT), από παρόχους δικτύων και υπηρεσιών ηλεκτρονικών επικοινωνιών και από παρόχους τεχνολογιών και υπηρεσιών ασφάλειας, αποτελεί έννομο συμφέρον του ενδιαφερόμενου υπευθύνου επεξεργασίας δεδομένων. Αυτό θα μπορούσε να περιλαμβάνει, λόγου χάρη, την αποτροπή ανεξουσιοδότητης πρόσβασης σε δίκτυα ηλεκτρονικών επικοινωνιών και διανομής κακόβουλων κωδικών και την παύση επιθέσεων «άρνησης υπηρεσίας» και ζημιών σε συστήματα πληροφορικής και ηλεκτρονικών επικοινωνιών.

Αιτιολογική σκέψη (50)

Η επεξεργασία δεδομένων προσωπικού χαρακτήρα για σκοπούς άλλους από εκείνους για τους οποίους τα δεδομένα προσωπικού χαρακτήρα συλλέχθηκαν αρχικά θα πρέπει

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

να επιτρέπεται μόνο εφόσον η επεξεργασία είναι συμβατή με τους σκοπούς για τους οποίους τα δεδομένα προσωπικού χαρακτήρα συλλέχθηκαν αρχικά. Σε αυτήν την περίπτωση, δεν απαιτείται νομική βάση χωριστή από εκείνη που επέτρεψε τη συλλογή των δεδομένων προσωπικού χαρακτήρα. Εάν η επεξεργασία είναι αναγκαία για την εκπλήρωση καθήκοντος που εκτελείται προς το δημόσιο συμφέρον ή κατά την άσκηση δημόσιας εξουσίας που έχει ανατεθεί στον υπεύθυνο επεξεργασίας, το δίκαιο της Ένωσης ή κράτους μέλους μπορεί να καθορίζει και να προσδιορίζει τα καθήκοντα και τους σκοπούς για τους οποίους πρέπει να θεωρείται συμβατή και σύννομη η περαιτέρω επεξεργασία. Η περαιτέρω επεξεργασία για λόγους αρχειοθέτησης που άπτονται του δημόσιου συμφέροντος, για σκοπούς επιστημονικής ή ιστορικής έρευνας ή για στατιστικούς σκοπούς θα πρέπει να θεωρείται συμβατή σύννομη πράξη επεξεργασίας. Η νομική βάση που προβλέπεται από το δίκαιο της Ένωσης ή κράτους μέλους για την επεξεργασία των δεδομένων προσωπικού χαρακτήρα μπορεί επίσης να συνιστά τη νομική βάση για την περαιτέρω επεξεργασία. Για να εξακριβωθεί αν ο σκοπός της περαιτέρω επεξεργασίας είναι συμβατός με τον σκοπό της αρχικής συλλογής των δεδομένων προσωπικού χαρακτήρα, ο υπεύθυνος επεξεργασίας, εφόσον πληροί όλες τις απαιτήσεις για τη νομιμότητα της αρχικής επεξεργασίας, θα πρέπει να λάβει υπόψη, μεταξύ άλλων: τυχόν συνδέσμους μεταξύ των σκοπών αυτών και των σκοπών της επιδιωκόμενης περαιτέρω επεξεργασίας· το πλαίσιο στο οποίο έχουν συλλεγεί τα δεδομένα προσωπικού χαρακτήρα, ιδίως τις εύλογες προσδοκίες του υποκειμένου των δεδομένων βάσει της σχέσης του με τον υπεύθυνο επεξεργασίας ως προς την περαιτέρω χρήση τους· τη φύση των δεδομένων προσωπικού χαρακτήρα· τις συνέπειες της επιδιωκόμενης περαιτέρω επεξεργασίας για τα υποκείμενα των δεδομένων· και την ύπαρξη κατάλληλων εγγυήσεων τόσο για τις αρχικές όσο και τις σκοπούμενες πράξεις περαιτέρω επεξεργασίας.

Όταν το υποκείμενο των δεδομένων παρέσχε τη συναίνεσή του ή η επεξεργασία βασίζεται στο δίκαιο της Ένωσης ή κράτους μέλους που συνιστά αναγκαίο και αναλογικό μέτρο σε μια δημοκρατική κοινωνία για τη διασφάλιση, ειδικότερα, σημαντικών σκοπών στο πλαίσιο γενικού δημόσιου συμφέροντος, θα πρέπει να επιτρέπεται στον υπεύθυνο επεξεργασία να προβαίνει στην περαιτέρω επεξεργασία των δεδομένων προσωπικού χαρακτήρα, ανεξάρτητα από τη συμβατότητα των σκοπών. Σε κάθε περίπτωση, θα πρέπει να διασφαλίζεται η εφαρμογή των αρχών που καθορίζονται στον παρόντα κανονισμό και, ιδίως, η ενημέρωση του υποκειμένου των δεδομένων σχετικά με τους άλλους αυτούς σκοπούς και σχετικά με τα δικαιώματά του, συμπεριλαμβανομένου του δικαιώματος προβολής αντιρρήσεων. Η επισήμανση πιθανών εγκληματικών πράξεων ή απειλών κατά της δημόσιας ασφάλειας από τον υπεύθυνο επεξεργασίας και η διαβίβαση των σχετικών δεδομένων προσωπικού

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

χαρακτήρα σε αρμόδια αρχή σε μία μεμονωμένη υπόθεση ή σε περισσότερες από μία υποθέσεις που αφορούν την ίδια αξιόποινη πράξη ή τις ίδιες απειλές για τη δημόσια ασφάλεια θα πρέπει να θεωρείται ως εμπίπτουσα στο πλαίσιο του θεμιτού συμφέροντος που επιδιώκει ο υπεύθυνος επεξεργασίας. Ωστόσο, η διαβίβαση αυτή στο πλαίσιο του θεμιτού συμφέροντος του υπευθύνου επεξεργασίας ή η περαιτέρω επεξεργασία δεδομένων προσωπικού χαρακτήρα θα πρέπει να απαγορεύεται, εάν η επεξεργασία δεν είναι συμβατή με νομική, επαγγελματική ή άλλη δεσμευτική υποχρέωση τήρησης απορρήτου.

Άρθρο 4

Ορισμοί

Για τους σκοπούς του παρόντος κανονισμού νοούνται ως:

[…]

(11) «συγκατάθεση» του υποκειμένου των δεδομένων: ***κάθε ένδειξη βουλήσεως, ελεύθερη, συγκεκριμένη, ρητή και εν πλήρει επιγνώσει, με την οποία το υποκείμενο των δεδομένων εκδηλώνει ότι συμφωνεί, με δήλωση ή με σαφή θετική ενέργεια, να αποτελέσουν αντικείμενο επεξεργασίας τα δεδομένα προσωπικού χαρακτήρα που το αφορούν***

Άρθρο 6

Νομιμότητα της επεξεργασίας

1. *Η επεξεργασία είναι σύννομη μόνο εάν και εφόσον ισχύει* ***τουλάχιστον μία από τις ακόλουθες προϋποθέσεις:***

(α) το υποκείμενο των δεδομένων έχει συναινέσει στην επεξεργασία των δεδομένων προσωπικού χαρακτήρα του για έναν ή περισσότερους συγκεκριμένους σκοπούς,

(β) η επεξεργασία είναι απαραίτητη για την εκτέλεση σύμβασης της οποίας το υποκείμενο των δεδομένων είναι συμβαλλόμενο μέρος ή για να ληφθούν μέτρα κατ' αίτηση του υποκειμένου των δεδομένων πριν από τη σύναψη σύμβασης,

(γ) η επεξεργασία είναι απαραίτητη για τη συμμόρφωση με έννομη υποχρέωση του υπευθύνου επεξεργασίας,

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

(δ) η επεξεργασία είναι απαραίτητη για τη διαφύλαξη ζωτικού συμφέροντος του υποκειμένου των δεδομένων ή άλλου φυσικού προσώπου,

(ε) η επεξεργασία είναι απαραίτητη για την εκπλήρωση καθήκοντος που εκτελείται προς το δημόσιο συμφέρον ή κατά την άσκηση δημόσιας εξουσίας που έχει ανατεθεί στον υπεύθυνο επεξεργασίας,

(στ) η επεξεργασία είναι απαραίτητη για τους σκοπούς των έννομων συμφερόντων που επιδιώκει ο υπεύθυνος επεξεργασίας ή τρίτος, εκτός εάν έναντι των συμφερόντων αυτών υπερισχύει το συμφέρον ή τα θεμελιώδη δικαιώματα και οι ελευθερίες του υποκειμένου των δεδομένων που επιβάλλουν την προστασία των δεδομένων προσωπικού χαρακτήρα, ιδίως εάν το υποκείμενο των δεδομένων είναι παιδί.

Το στοιχείο στ) του πρώτου εδαφίου δεν εφαρμόζεται στην επεξεργασία που διενεργείται από δημόσιες αρχές κατά την άσκηση των καθηκόντων τους.

2. Τα κράτη μέλη μπορούν να διατηρούν ή να θεσπίζουν πιο ειδικές διατάξεις για την προσαρμογή της εφαρμογής των κανόνων του παρόντος κανονισμού όσον αφορά την επεξεργασία για τη συμμόρφωση με την παράγραφο 1 στοιχεία γ) και ε), καθορίζοντας ακριβέστερα ειδικές απαιτήσεις για την επεξεργασία και άλλα μέτρα προς εξασφάλιση σύννομης και θεμιτής επεξεργασίας, μεταξύ άλλων για άλλες ειδικές περιπτώσεις επεξεργασίας όπως προβλέπονται στο κεφάλαιο IX.

3. Η βάση για την επεξεργασία που αναφέρεται στην παράγραφο 1 στοιχείο γ) και:

(α) το δίκαιο της Ένωσης, ή

(β) το δίκαιο του κράτους μέλος στο οποίο υπόκειται ο υπεύθυνος επεξεργασίας.

Ο σκοπός της επεξεργασίας καθορίζεται στην εν λόγω νομική βάση ή, όσον αφορά την επεξεργασία που αναφέρεται στην παράγραφο 1 στοιχείο ε), είναι η αναγκαιότητα της επεξεργασίας για την εκπλήρωση καθήκοντος που εκτελείται προς το δημόσιο συμφέρον ή κατά την άσκηση δημόσιας εξουσίας που έχει ανατεθεί στον υπεύθυνο επεξεργασίας. Η εν λόγω νομική βάση μπορεί να περιλαμβάνει ειδικές διατάξεις για την προσαρμογή της εφαρμογής των κανόνων του παρόντος κανονισμού, μεταξύ άλλων: τις γενικές προϋποθέσεις που διέπουν τη σύννομη επεξεργασία από τον υπεύθυνο επεξεργασίας· τα είδη των δεδομένων που υποβάλλονται σε επεξεργασία· τα οικεία υποκείμενα των δεδομένων· τις οντότητες στις οποίες μπορούν να κοινοποιούνται τα δεδομένα προσωπικού χαρακτήρα και τους σκοπούς αυτής της κοινοποίησης· τον περιορισμό του σκοπού· τις περιόδους αποθήκευσης· και τις πράξεις επεξεργασίας και τις διαδικασίες επεξεργασίας, συμπεριλαμβανομένων των

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

μέτρων για τη διασφάλιση σύννομης και θεμιτής επεξεργασίας, όπως εκείνα για άλλες ειδικές περιπτώσεις επεξεργασίας όπως προβλέπονται στο κεφάλαιο IX. Το δίκαιο της Ένωσης ή το δίκαιο του κράτους μέλους ανταποκρίνεται σε σκοπό δημόσιου συμφέροντος και είναι ανάλογο προς τον επιδιωκόμενο νόμιμο σκοπό.

4. Όταν η επεξεργασία για σκοπό άλλο από αυτόν για τον οποίο έχουν συλλεγεί τα δεδομένα προσωπικού χαρακτήρα δεν βασίζεται στη συγκατάθεση του υποκειμένου των δεδομένων ή στο δίκαιο της Ένωσης ή το δίκαιο κράτους μέλους το οποίο αποτελεί αναγκαίο και αναλογικό μέτρο σε μια δημοκρατική κοινωνία για τη διασφάλιση των σκοπών που αναφέρονται στο άρθρο 23 παράγραφος 1, ο υπεύθυνος επεξεργασίας, προκειμένου να εξακριβωθεί κατά πόσο η επεξεργασία για άλλο σκοπό είναι συμβατή με τον σκοπό για τον οποίο συλλέγονται αρχικώς τα δεδομένα προσωπικού χαρακτήρα, λαμβάνει υπόψη, μεταξύ άλλων:

(α) τυχόν σχέση μεταξύ των σκοπών για τους οποίους έχουν συλλεχθεί τα δεδομένα προσωπικού χαρακτήρα και των σκοπών της επιδιωκόμενης περαιτέρω επεξεργασίας,

(β) το πλαίσιο εντός του οποίου συλλέχθηκαν τα δεδομένα προσωπικού χαρακτήρα, ιδίως όσον αφορά τη σχέση μεταξύ των υποκειμένων των δεδομένων και του υπευθύνου επεξεργασίας,

(γ) τη φύση των δεδομένων προσωπικού χαρακτήρα, ιδίως για τις ειδικές κατηγορίες δεδομένων προσωπικού χαρακτήρα που υποβάλλονται σε επεξεργασία, σύμφωνα με το άρθρο 9, ή κατά πόσο δεδομένα προσωπικού χαρακτήρα που σχετίζονται με ποινικές καταδίκες και αδικήματα υποβάλλονται σε επεξεργασία, σύμφωνα με το άρθρο 10,

(δ) τις πιθανές συνέπειες της επιδιωκόμενης περαιτέρω επεξεργασίας για τα υποκείμενα των δεδομένων,

(ε) την ύπαρξη κατάλληλων εγγυήσεων, που μπορεί να περιλαμβάνουν κρυπτογράφηση ή ψευδωνυμοποίηση.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

2. ΝΟΜΙΚΟΙ ΛΟΓΟΙ ΓΙΑ ΤΗΝ ΕΠΕΞΕΡΓΑΣΙΑ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ ΣΤΟ ΠΛΑΙΣΙΟ ΤΟΥ ΓΚΠΔ (ΓΕΝΙΚΟΥ ΚΑΝΟΝΙΣΜΟΥ ΓΙΑ ΤΗΝ ΠΡΟΣΤΑΣΙΑ ΤΩΝ ΔΕΔΟΜΕΝΩΝ)

2.1. Συγκατάθεση

2.1.1. Σημασία και νομικές απαιτήσεις

Η συγκατάθεση είναι ένας από τους έξι νομικούς λόγους που απαριθμούνται στο άρθρο. 6 του ΓΚΠΔ. Προκειμένου να είναι έγκυρη, το ΓΚΠΔ απαιτεί η συγκατάθεση να παρέχεται ελεύθερα, να είναι συγκεκριμένη, ρητή, και εν πλήρει επιγνώσει.

- **«ελεύθερη»=** συνεπάγεται πραγματική επιλογή και έλεγχο για τα πρόσωπα στα οποία αναφέρονται τα δεδομένα[i]. Εάν προκύψουν δυσμενείς συνέπειες για το υποκείμενο των δεδομένων, σε περίπτωση που δεν συγκατατεθούν για την επεξεργασία / απόσυρση της ήδη δοθείσας συναίνεσης (π.χ. άρνηση παροχής υπηρεσιών, υψηλότερο κόστος για αγαθά / υπηρεσίες - τέλη, τιμή κλπ.), η συγκατάθεση πρέπει να θεωρείται ότι δεν έχει δοθεί ελεύθερα. Λόγω της ανισότητας των εξουσιών μεταξύ των δημοσίων αρχών και των προσώπων στα οποία αναφέρονται τα δεδομένα, η συγκατάθεση σπανίως θα είναι χρήσιμο εργαλείο για την επεξεργασία δεδομένων στο πλαίσιο άσκησης των επίσημων αρχών.
- **«συγκεκριμένη»=** στενά συνδεδεμένη με την απαίτηση ότι το υποκείμενο των δεδομένων συναινεί για έναν ή περισσότερους ειδικούς σκοπούς της επεξεργασίας (αποκαλούμενη ως «λεπτομερειακότητα» της συγκατάθεσης[ii]) και τον σκοπό της αρχής της προδιαγραφής. Κάθε ένας από τους σκοπούς της επεξεργασίας δεδομένων πρέπει να καθοριστεί με σαφήνεια από την αρχή πριν από το υποκείμενο των δεδομένων. Το υποκείμενο των δεδομένων θα πρέπει να έχει τη δυνατότητα να επιλέγει για ποιους σκοπούς παρέχει την συναίνεσή του (π.χ. να συναινέσει για τους σκοπούς Α, Β και Γ και να μην δώσει συγκατάθεση για τους σκοπούς Ε και Δ). Οι πληροφορίες σχετικά με τη συγκατάθεση πρέπει να διαχωρίζονται σαφώς από τις πληροφορίες που σχετίζονται με οποιοδήποτε άλλο θέμα. Πρέπει να υπάρχει συγκατάθεση για κάθε νέο σκοπό επεξεργασίας και οι ελεγκτές θα πρέπει να παρέχουν συγκεκριμένες πληροφορίες με κάθε ξεχωριστό αίτημα συγκατάθεσης σχετικά με τα δεδομένα που υποβάλλονται σε επεξεργασία για κάθε σκοπό.
- **"εν πλήρει επιγνώσει"=** οι ελάχιστες απαιτήσεις βάσει του ΓΚΠΔ περιλαμβάνουν την παροχή πληροφοριών για τον υπεύθυνο επεξεργασίας δεδομένων και τους σκοπούς της επεξεργασίας. Η ομάδα εργασίας του άρθρου 29 (WP29) συνιστά τη

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

συμπερίληψη πρόσθετων πληροφοριών, όπως είναι ο τύπος των δεδομένων που συλλέγονται και χρησιμοποιούνται· το δικαίωμα απόσυρσης της συναίνεσης· πληροφορίες σχετικά με τη χρήση των δεδομένων για αποφάσεις που βασίζονται αποκλειστικά σε αυτοματοποιημένη επεξεργασία, συμπεριλαμβανομένης της μορφοποίησης[iii]; · σε περίπτωση μεταφορών - πληροφορίες σχετικά με τους ενδεχόμενους κινδύνους μεταφοράς δεδομένων σε τρίτες χώρες ελλείψει απόφασης επάρκειας και κατάλληλων διασφαλίσεων[iv].

- **«Ρητή» =** η συγκατάθεση πρέπει να δίνεται μέσω δήλωσης του υποκειμένου των δεδομένων ή μιας σαφούς καταφατικής πράξης. Η συγκατάθεση πρέπει πάντα να δίνεται με ενεργητική κίνηση ή δήλωση. Έτσι, η σιωπή, τα προσυμπληρωμένα τετραγωνίδια ή η αδράνεια δεν θα πρέπει να εκλαμβάνονται ως συγκατάθεση στο πλαίσιο του ΓΚΠΔ.
- **Να μπορεί να αποσυρθεί με την ίδια ευκολία που δόθηκε=** η συγκατάθεση θα μπορούσε να ανακληθεί ανά πάσα στιγμή. Αυτό δεν πρέπει να συμβαίνει κατ 'ανάγκη με την ίδια ενέργεια, αλλά η διαδικασία απόσυρσης πρέπει να είναι τόσο εύκολη όσο και η διαδικασία της συγκατάθεσης. (π.χ. κάνοντας κλικ σε ένα πλαίσιο στη διαδικτυακή δήλωση με τη συγκατάθεσή σας για να λάβετε την εφημερίδα του δήμου, είναι τόσο εύκολο όσο κάνοντας κλικ σε ένα σύνδεσμο στο σώμα του μηνύματος που συνοδεύει το ενημερωτικό δελτίο για διαγραφή και απόσυρση της συγκατάθεσης);
- Ειδικές απαιτήσεις σχετικά με τη συγκατάθεση που προέρχεται από παιδιά= Ο ΓΚΠΔ αντιμετωπίζει τα παιδιά ως ευπαθή κατηγορία υποκειμένων δεδομένων. Τα παιδιά απαιτούν ειδική προστασία όσον αφορά τα δεδομένα προσωπικού χαρακτήρα, καθώς μπορεί να έχουν μικρότερη επίγνωση των σχετικών κινδύνων, συνεπειών και εγγυήσεων των δικαιωμάτων τους σε σχέση με την επεξεργασία δεδομένων προσωπικού χαρακτήρα. Σε περίπτωση παροχής υπηρεσιών για την κοινωνία της πληροφορίας που προσφέρονται σε ένα παιδί (π.χ. ηλεκτρονικές εκπαιδευτικές εκστρατείες που διενεργούνται σε δικτυακούς τόπους των δήμων και απαιτούν συλλογή προσωπικών δεδομένων παιδιών), η συγκατάθεση για την επεξεργασία δεδομένων παιδιού κάτω των 16 ετών (τα κράτη μέλη μπορούν να μειώσουν την ηλικία έως τα 13 έτη) θα πρέπει να λαμβάνεται ή να εγκρίνεται από τον γονέα/κηδεμόνα του παιδιού·
- **Η συγκατάθεση βάσει της οδηγίας 95/46** = η συναίνεση που έχει ήδη αποκτηθεί βάσει του παλαιού καθεστώτος δεν θα πρέπει απαραίτητα να αναθεωρηθεί. Εάν η συγκατάθεση ανταποκρίνεται στις απαιτήσεις που ορίζονται στο ΓΚΠΔ, τότε η συναίνεση που αποκτάται βάσει της οδηγίας θα πρέπει να εξακολουθήσει να είναι βάσιμος λόγος για την επεξεργασία.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

Ο ελεγκτής δεδομένων είναι υπεύθυνος να αποδείξει ότι η συγκατάθεση έχει ληφθεί δεόντως[v].

2.1.2. Εφαρμογή στο πλαίσιο της δραστηριότητας των Τοπικών Αρχών

Στην πράξη, η συγκατάθεση σπάνια θα είναι το βασικό νομικό πλαίσιο στο οποίο οι τοπικές αρχές θα επεξεργάζονται νόμιμα τα προσωπικά δεδομένα των πολιτών. Το συμπέρασμα αυτό απορρέει από τις απαιτήσεις της ΓΚΠΔ, τις οποίες πρέπει να πληρούν οι συγκαταθέσεις για να είναι έγκυρες.

Πρώτον, το γεγονός ότι η συναίνεση πρέπει να παρέχεται «ελεύθερα», δηλαδή ότι δεν πρέπει να προκαλούνται αρνητικές συνέπειες στο υποκείμενο των δεδομένων σε περίπτωση που δεν δώσει την συναίνεση του, σημαίνει ότι σε κάθε περίπτωση κατά την οποία μια συγκεκριμένη Τοπική Αρχή ενεργεί ως κάτοχος δημόσιας εξουσίας, η συγκατάθεση να μην χρησιμοποιείται ως έγκυρη νομική βάση για την επεξεργασία. Ο έλεγχος για την ορθή εκτέλεση των δημόσιων υποχρεώσεων των πολιτών (π.χ. είσπραξη τοπικών τελών και φόρων, εγγραφή απόκτησης ακινήτων / οχημάτων κ.λπ.) και η επιβολή κυρώσεων σε περίπτωση μη εκτέλεσης τέτοιων υποχρεώσεων είναι εγγενώς συνδεδεμένη με το δικαίωμα (και την υποχρέωση) να ασκεί εξαναγκαστικές εξουσίες. Αυτό σημαίνει ότι τα υποκείμενα των δεδομένων δεν έχουν πραγματικά ελεύθερη επιλογή να συναινέσουν ή να μην συναινέσουν για την επεξεργασία των προσωπικών τους δεδομένων. Βρίσκονται σε δευτερεύουσα θέση και υποχρεούνται από το νόμο να συνεργάζονται με την Τοπική Αρχή.

Δεύτερον, η συγκατάθεση θα μπορούσε να αποσυρθεί «ανά πάσα στιγμή». Εάν η συναίνεση ήταν ο θεμιτός λόγος για την επεξεργασία των δεδομένων προσωπικού χαρακτήρα σε περίπτωση που οι πολίτες εκπληρώνουν τις νομικές υποχρεώσεις τους, ενδεχομένως οποιοσδήποτε κακόπιστος πολίτης (π.χ. μη πρόθυμος να εκπληρώσει ορισμένες δημόσιες υποχρεώσεις) θα μπορούσε να ανακαλέσει τη συναίνεσή του ανά πάσα στιγμή και θα μπορούσε να χρησιμοποιήσει αυτήν την απόσυρση ώστε να δημιουργήσει εμπόδια (και στην πράξη «να παρεμποδίσει») την κανονική λειτουργία της Τοπικής Αρχής. Σε περίπτωση ανάκλησης της συγκατάθεσης, η LA ως υπεύθυνος επεξεργασίας θα πρέπει να τερματίσει την επεξεργασία. Αυτό είναι αδιανόητο κατά την άσκηση των επίσημων αρχών, διότι θα θέσει σε κίνδυνο ολόκληρη την ιδέα της άσκησης δημόσιας εξουσίας.

Έτσι, στις καταστάσεις που περιγράφονται παραπάνω, η συγκατάθεση δεν είναι το σωστό εργαλείο για τέτοιου είδους επεξεργασία.

Σύμφωνα με το WP29, «η χρήση της συγκατάθεσης ως νόμιμης βάσης για την επεξεργασία δεδομένων από τις δημόσιες αρχές δεν εξαιρείται εντελώς από το νομικό

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

πλαίσιο του ΓΚΠΔ»[vi]. Συνεπώς, η συγκατάθεση μπορεί να είναι χρήσιμο εργαλείο σε περιπτώσεις στις οποίες η Τοπική Αρχή είτε δεν ασκεί τις τυπικές και κύριες λειτουργίες της είτε η αντίστοιχη επεξεργασία είναι μάλλον προαιρετική (και υπάρχουν διαδικασίες προεπιλογής επεξεργασίας που θα πραγματοποιηθούν σε περίπτωση που το υποκείμενο των δεδομένων δεν εγκρίνει). Παραδείγματα είναι οι ακόλουθες περιπτώσεις:

- Οι Τοπικές και Κυβερνητικές Αρχές απαιτούν τις ίδιες πληροφορίες για την έκδοση ορισμένων νομικών πράξεων κατόπιν αιτήματος ενός πολίτη, αλλά δεν είναι σε θέση να έχουν πρόσβαση ο ένας στις βάσεις δεδομένων του άλλου. Καθώς και οι δύο ζητούν τις ίδιες πληροφορίες από τον πολίτη, θα μπορούσαν να ζητήσουν τη συγκατάθεση του πολίτη για τη συγχώνευση των φακέλων, για να αποφευχθούν διπλές διαδικασίες και αλληλογραφία. Και οι δύο δημόσιοι φορείς θα πρέπει να διασφαλίσουν ότι αυτό είναι προαιρετικό και ότι η έκδοση του εγγράφου θα εξασφαλίζεται ακόμη και αν ο πολίτης δεν συμφωνεί με τη συγχώνευση των δεδομένων[vii];
- Οι Τοπικές Αρχές προβλέπουν τη δυνατότητα ενημέρωσης των πολιτών που συμμετέχουν διοικητικές διαδικασίες που τους αφορούν, μέσω ηλεκτρονικού ταχυδρομείου. Το καθεστώς είναι opt-in, δηλ. Οι πολίτες είναι ελεύθεροι να αποφασίσουν εάν θα ειδοποιηθούν μέσω ηλεκτρονικού ταχυδρομείου (π.χ. σημειώνοντας το κουτί σε ηλεκτρονική / έντυπη μορφή και παρέχοντας το email τους). Σε περίπτωση άρνησης συγκατάθεσης / ανάκλησης της συναίνεσης, η Τοπική Αρχή θα πρέπει να έχει μια προεπιλεγμένη διαδικασία για την κοινοποίηση (π.χ. με συστημένη επιστολή). Η επεξεργασία του μηνύματος ηλεκτρονικού ταχυδρομείου σε μια τέτοια περίπτωση θα βασίζεται στη συναίνεση.
- Η Τοπική Αρχή παρέχει στους πολίτες τη δυνατότητα να εγγραφούν για να λαμβάνουν προσκλήσεις για διάφορες δραστηριότητες που διοργανώνει η ίδια (π.χ. εκθέσεις σε τοπικά μουσεία, θεατρικές πρεμιέρες στο δημοτικό θέατρο, εκστρατείες συλλογής απορριμμάτων, διαγωνισμοί / εκπαιδευτικές εκστρατείες που διεξάγονται στα δημοτικά σχολεία). Η συνδρομή απαιτεί την παροχή δεδομένων επικοινωνίας (π.χ. ταχυδρομική διεύθυνση, αριθμό τηλεφώνου, ηλεκτρονικό ταχυδρομείο κ.λπ.) καθώς και δεδομένα για τις προτιμήσεις των υποκειμένων των δεδομένων (π.χ. χόμπι, ενδιαφέροντα κ.λπ.). Η επεξεργασία τέτοιων δεδομένων θα βασίζεται στη συναίνεση, καθώς οι πολίτες δικαιούνται να διαγραφούν από αυτές τις ειδοποιήσεις ελεύθερα ανά πάσα στιγμή, χωρίς αρνητικές συνέπειες.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

2.2. Εκτέλεση / σύναψη σύμβασης με το υποκείμενο των δεδομένων

2.2.1. Σημασία & νομικές απαιτήσεις

Η διάταξη του άρθρου. 6, παράγραφος 1, στοιχείο "β" του ΓΚΠΔ εισάγει δύο χωριστούς νομικούς λόγους για την επεξεργασία προσωπικών δεδομένων:

(i) καταστάσεις όπου η επεξεργασία είναι απαραίτητη για την εκτέλεση της σύμβασης στην οποία το πρόσωπο στο οποίο αναφέρονται τα δεδομένα είναι μέλος

(ii) καταστάσεις όπου η επεξεργασία πραγματοποιείται πριν από τη σύναψη της σύμβασης. Αυτό καλύπτει τις προσυμβατικές σχέσεις, υπό τον όρο ότι λαμβάνονται μέτρα κατόπιν αιτήματος του υποκειμένου των δεδομένων και όχι με πρωτοβουλία του υπεύθυνου επεξεργασίας ή τρίτου μέλους[viii].

Η πρώτη υπόθεση πρέπει να ερμηνεύεται αυστηρά και δεν πρέπει να καλύπτει καταστάσεις όπου η επεξεργασία δεν είναι πραγματικά αναγκαία για την εκτέλεση μιας σύμβασης, αλλά επιβάλλεται μονομερώς στο πρόσωπο στο οποίο αναφέρονται τα δεδομένα από τον υπεύθυνο επεξεργασίας[ix]. Σύμφωνα με την ερμηνεία που δόθηκε από το WP29 για τον ίδιο λόγο βάσει της παλαιάς οδηγίας 95/46, ο παραπάνω νομικός λόγος εφαρμόζεται μόνο σε ό, τι είναι απαραίτητο για την εκτέλεση της σύμβασης. Με άλλα λόγια, εφόσον η επεξεργασία καλύπτει την κανονική εκτέλεση μιας σύμβασης, θα μπορούσε να εμπίπτει στην εν λόγω νομική βάση. Αυτός ο νομικός λόγος θα καλύπτει καταστάσεις κατά τις οποίες η επεξεργασία πραγματοποιείται στο πλαίσιο σύμβασης ανεξαρτήτως της φάσης της σύμβασης[x]. Ωστόσο, οι τυχόν περαιτέρω ενέργειες που προκαλούνται από τη μη συμμόρφωση ή σε όλα τα άλλα περιστατικά κατά την εκτέλεση μιας σύμβασης δεν εμπίπτουν στο πεδίο εφαρμογής αυτού του νομικού πλαισίου. Αυτοί οι τύποι επεξεργασίας θα απαιτούσαν την εφαρμογή διαφορετικών νομικών βάσεων - π.χ. υπερισχύον έννομο συμφέρον του υπεύθυνου επεξεργασίας δεδομένων.

Η δεύτερη υπόθεση θα μπορούσε να περιλαμβάνει την επεξεργασία που απαιτείται για την προετοιμασία των προσφορών, τις προσλήψεις για δραστηριότητες Ανθρώπινου Δυναμικού κλπ. Ωστόσο, οποιοιδήποτε λεπτομερείς έλεγχοι ιστορικού των υποψηφίων θα ήταν αρκετά εκτενείς και δεν θα δικαιολογούνταν ως απαιτούμενα βήματα από το υποκείμενο των δεδομένων.

Γενικά, αυτός ο νομικός λόγος ερμηνεύεται στενά από τις ρυθμιστικές αρχές, οπότε οι ελεγκτές θα πρέπει να είναι σε θέση να αποδείξουν ότι η επεξεργασία είναι αναπόφευκτη για την ολοκλήρωση της σύμβασης[xi].

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

2.2.2. Εφαρμογή στο πλαίσιο της δραστηριότητας των Τοπικών Αρχών

Αυτός ο νομικός λόγος για την επεξεργασία δεδομένων προσωπικού χαρακτήρα θα μπορούσε να εφαρμοστεί από τις Τοπικές Αρχές τουλάχιστον στους ακόλουθους τομείς:

- Επεξεργασία στο πλαίσιο της απασχόλησης - π.χ. επεξεργασία πληροφοριών μισθοδοσίας και στοιχεία τραπεζικού λογαριασμού, έτσι ώστε να καταβάλλονται οι μισθοί[xii];
- Επεξεργασία στο πλαίσιο της σύναψης συμβάσεων για δημόσιες προμήθειες - αυτός ο συμβατικός νομικός λόγος θα μπορούσε να επικαλυφθεί με ένα άλλο νομικό υπόβαθρο για την επεξεργασία δεδομένων προσωπικού χαρακτήρα - π.χ. τη νομική υποχρέωση της Τοπικής Αρχής για επεξεργασία δεδομένων προσωπικού χαρακτήρα στο πλαίσιο της αντίστοιχης διοικητικής διαδικασίας που επιβάλλει ο τοπικός νόμος ·
- Επεξεργασία στο πλαίσιο των σχέσεων μεταξύ ορισμένων ιδιωτικών οντοτήτων που ανήκουν εξ ολοκλήρου / εν μέρει στον δήμο / κράτος και τους πολίτες - π.χ. φορείς παροχής υπηρεσιών δημόσιας συγκοινωνίας σε ολόκληρη την πόλη / χωριό, φορείς που παρέχουν υπηρεσίες κοινής ωφέλειας (παροχή ηλεκτρισμού, φυσικού αερίου, ύδρευσης κ.λπ.) κατά τη σύναψη των αντίστοιχων συμβάσεων.

2.3. Νομική υποχρέωση

2.3.1. Σημασία & νομικές απαιτήσεις

Αυτός ο νομικός λόγος απαιτεί μια σαφή νομική διάταξη η οποία θα εισαχθεί είτε σε νομοθετικό είτε σε υποχωρητικό (το λεγόμενο δευτερογενές δίκαιο ορισμένων κρατών μελών) που υποχρεώνει τον υπεύθυνο επεξεργασίας να διεξάγει τη μεταποίηση. Το WP29 υπογραμμίζει ότι ο νόμος πρέπει να πληροί όλες τις σχετικές προϋποθέσεις ώστε η υποχρέωση να είναι έγκυρη και δεσμευτική και πρέπει επίσης να συμμορφώνεται με τη νομοθεσία περί προστασίας δεδομένων, συμπεριλαμβανομένης της απαίτησης αναγκαιότητας, αναλογικότητας και περιορισμού του σκοπού[xiii]. Ο ΓΚΠΔ απαιτεί ρητά ότι αυτή η υποχρέωση θα πρέπει να είναι:

(i) υποχρέωση του κράτους μέλους ή της νομοθεσίας της ΕΕ στην οποία υπόκειται ο υπεύθυνος επεξεργασίας. Το WP29 έχει ήδη κάνει την ακόλουθη ερμηνεία στο πλαίσιο της παλαιάς οδηγίας 95/46 σχετικά: οι υποχρεώσεις που απορρέουν από τη νομοθεσία τρίτων χωρών (όπως για παράδειγμα η υποχρέωση θέσπισης συστημάτων καταγγελίας δυσλειτουργιών βάσει του νόμου Sarbanes-Oxley του 2002 στις Ηνωμένες Πολιτείες) δεν καλύπτονται από τη νομική υποχρέωση. Για να είναι έγκυρη, μια νομική υποχρέωση μιας

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

τρίτης χώρας θα πρέπει να αναγνωριστεί επισήμως και να ενσωματωθεί στην έννομη τάξη του ενδιαφερόμενου κράτους μέλους, π.χ. υπό τη μορφή διεθνούς συμφωνίας · και

(ii) «σαφής και ακριβής» και η εφαρμογή της να είναι προβλέψιμη για όσους υπόκεινται σε αυτήν. Οι αιτιολογικές σκέψεις 41 και 45 του ΓΚΠΔ καθιστούν σαφές ότι η σχετική «νομική υποχρέωση» δεν είναι υποχρεωτική, όπου θα μπορούσε να έχει πρακτικές συνέπειες για τις χώρες του κοινού δικαίου - θα ήταν αρκετό, αν πληρούσε τη «σαφή και ακριβή» δοκιμή. Μια νομική υποχρέωση θα μπορούσε να καλύψει διάφορες δραστηριότητες επεξεργασίας που πραγματοποιήθηκαν από τον υπεύθυνο επεξεργασίας, ώστε να μην είναι απαραίτητο να προσδιοριστεί μια συγκεκριμένη νομική υποχρέωση για κάθε μεμονωμένη δραστηριότητα επεξεργασίας[xiv].

Το WP29 έχει αναφέρει ότι για να εφαρμοστεί αυτός ο νομικός λόγος, ο υπεύθυνος της επεξεργασίας δεν πρέπει να έχει την επιλογή να εκπληρώσει ή όχι την υποχρέωση. Οι εθελοντικές μονομερείς δεσμεύσεις και οι εταιρικές σχέσεις δημόσιου και ιδιωτικού τομέα που επεξεργάζονται δεδομένα πέρα από τα όσα απαιτεί ο νόμος δεν καλύπτονται από αυτό το νομικό υπόβαθρο[xv]. Η νομική υποχρέωση ως λόγος επεξεργασίας δεδομένων προσωπικού χαρακτήρα πρέπει να εφαρμόζεται βάσει νομικών διατάξεων που αναφέρονται ρητώς στη φύση και το αντικείμενο της επεξεργασίας. Ο υπεύθυνος επεξεργασίας δεν θα πρέπει να διαθέτει αδικαιολόγητο βαθμό διακριτικής ευχέρειας όσον αφορά τον τρόπο συμμόρφωσης με τη νομική υποχρέωση[xvi].

Το WP29 αναγνωρίζει ρητά ότι η νομοθεσία μπορεί σε ορισμένες περιπτώσεις να θέτει μόνο έναν γενικό στόχο, ενώ πιο συγκεκριμένες υποχρεώσεις επιβάλλονται σε διαφορετικό επίπεδο (π.χ. στο παράγωγο δίκαιο ή σε δεσμευτική απόφαση δημόσιας αρχής). Σύμφωνα με το WP29, αυτό μπορεί επίσης να οδηγήσει σε νομικές υποχρεώσεις υπό τον όρο ότι η φύση και το αντικείμενο της επεξεργασίας καθορίζονται σαφώς και υπόκεινται σε επαρκή νομική βάση[xvii].

2.3.2. Εφαρμογή στο πλαίσιο της δραστηριότητας των Τοπικών Αρχών

Στην πράξη, αυτός ο νομικός λόγος θα ήταν ένας από τους σημαντικότερους νομικούς λόγους για την επεξεργασία προσωπικών δεδομένων που διεξήγαγαν οι Τοπικές Αρχές. Αυτός ο νομικός λόγος θα καλύπτει και τις δύο καταστάσεις που σχετίζονται με την παροχή διοικητικών υπηρεσιών / τη διευκόλυνση της εκπλήρωσης των δημοσίων υποχρεώσεων των πολιτών και την εκπλήρωση ορισμένων ειδικών υποχρεώσεων των Τοπικών Αρχών υπό την ιδιότητά τους ως εργοδότες. Αυτό το νομικό υπόβαθρο θα μπορούσε να εφαρμοστεί π.χ. στις ακόλουθες περιπτώσεις:

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

- συλλογή δεδομένων από την Τοπική Αρχή για τον χειρισμό κυρώσεων για στάθμευση σε μη εξουσιοδοτημένους χώρους.
- αναφορά των μισθών των υπαλλήλων της Τοπικής Αρχής σε ασφαλιστικές ή φορολογικές αρχές[xviii].

2.4. Ζωτικό συμφέρον

2.4.1. Σημασία & νομικές απαιτήσεις

Ο νομικός αυτός λόγος πρέπει να ερμηνεύεται πολύ στενά. Το WP29 έχει επίσης αναγνωρίσει ότι το ζωτικό συμφέρον πρέπει να έχει περιορισμένη εφαρμογή xix. Η έννοια του «ζωτικού συμφέροντος» συνδέεται εγγενώς με την επικείμενη απειλή για τα θεμελιώδη αγαθά του υποκειμένου των δεδομένων (ζωή, υγεία, σωματική ακεραιότητα κ.λπ.). Στο νομικό δόγμα υποδεικνύεται ότι η προβλεπόμενη επεξεργασία θα πρέπει να είναι ζωτικής σημασίας για την επιβίωση ενός ατόμουxx. Σύμφωνα με την ερμηνεία της WP29 στο πλαίσιο της παλιάς οδηγίας 95/46, η απειλή πρέπει να είναι άμεση, δηλαδή η συλλογή και επεξεργασία δεδομένων προσωπικού χαρακτήρα σε μεγάλη κλίμακα για καθαρά προληπτικούς σκοπούς δεν μπορεί να εμπίπτει στο πεδίο εφαρμογής αυτού του νομικού λόγουxxi. Η αιτιολογική σκέψη 46 του ΓΚΠΔ επιτρέπει ρητά τη διεκπεραίωση αυτού του νομικού λόγου για ανθρωπιστικούς σκοπούς, συμπεριλαμβανομένης της παρακολούθησης των επιδημιών και της εξάπλωσής τους ή σε καταστάσεις ανθρωπιστικών καταστάσεων έκτακτης ανάγκης, ιδίως σε καταστάσεις φυσικών και ανθρωπογενών καταστροφών (σε αυτά τα σενάρια μπορεί να επικαλύπτονται τόσο οι σημαντικοί λόγοι δημόσιου συμφέροντος όσο και το ζωτικό συμφέρον). Έτσι, αυτή η αυστηρή ερμηνεία που επιβάλλει το WP29 μπορεί να «μαλακώσει» στο μέλλον.

Πρέπει επίσης να σημειωθεί ότι, σύμφωνα με την παλιά οδηγία 95/46, το νομικό ζήτημα «ζωτικό συμφέρον» αφορούσε μόνο το συμφέρον του υποκειμένου των δεδομένων. Με τον ΓΚΠΔ το εύρος αυτού του νομικού εδάφους έχει ευρύτερο πεδίο - το ζωτικό συμφέρον μπορεί να είναι είτε το πρόσωπο στο οποίο αναφέρονται τα δεδομένα είτε άλλο φυσικό πρόσωπο. Ο ΓΚΠΔ απαιτεί ρητώς ότι η επεξεργασία δεδομένων προσωπικού χαρακτήρα με βάση το ζωτικό συμφέρον άλλου φυσικού προσώπου θα πρέπει καταρχήν να πραγματοποιείται μόνο όταν η επεξεργασία δεν μπορεί εμφανώς να βασίζεται σε άλλη νομική βάση. Με άλλα λόγια, η βασιζόμενη στο ζωτικό συμφέρον επεξεργασία θα αποτελούσε μάλλον λύση «έσχατης διεξόδου» για τους ελεγκτές.

2.4.2. Εφαρμογή στο πλαίσιο της δραστηριότητας των Τοπικών Αρχών

Η δυνατότητα εφαρμογής αυτού του λόγου στο πλαίσιο των δραστηριοτήτων της Τοπικής Αρχής είναι μάλλον περιορισμένη. Αυτός ο νομικός λόγος θα μπορούσε θεωρητικά να εφαρμοστεί σε πολύ περιορισμένο αριθμό περιπτώσεων, π.χ. για να δικαιολογηθεί η επεξεργασία προσωπικών δεδομένων των εργαζομένων ή των πολιτών σε περίπτωση

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

έκτακτης ανάγκης που σημειώθηκε εντός της δικαιοδοσίας της Τοπικής Αρχής και εφόσον δεν υπάρχει άλλος νομικός λόγος για την επεξεργασία αυτή (π.χ. νομική υποχρέωση ή άσκηση δημόσιας εξουσίας).

2.5. Δραστηριότητα που εκτελείται για το δημόσιο συμφέρον/άσκηση δημόσιας εξουσίας

2.5.1. Σημασία & νομικές απαιτήσεις

Το καθήκον ή η αρχή του υπευθύνου επεξεργασίας δεδομένων πρέπει να καθορίζεται από το δίκαιο της ΕΕ ή από το δίκαιο των κρατών μελών στο οποίο υπόκειται ο υπεύθυνος επεξεργασίας. Τα καθήκοντα που εκτελούνται για το δημόσιο συμφέρον μιας τρίτης χώρας ή για την άσκηση δημόσιας εξουσίας που χορηγείται βάσει του αλλοδαπού δικαίου δεν εμπίπτουν στο πεδίο εφαρμογής της παρούσας διάταξης στο πλαίσιο της παλαιάς οδηγίας 95/46[xxii] και η προσέγγιση αυτή συνεχίζεται με τον ΓΚΠΔ.

(i) όταν ο ίδιος ο υπεύθυνος επεξεργασίας έχει δημόσια εξουσία ή αποστολή δημοσίου συμφέροντος (αλλά δεν υποχρεούται απαραίτητα να επεξεργάζεται δεδομένα) και η επεξεργασία είναι αναγκαία για την άσκηση αυτής της εξουσίας ή για την εκτέλεση αυτής της αποστολής, ή

(ii) όταν ο υπεύθυνος επεξεργασίας δεν διαθέτει δημόσια αρχή αλλά ζητείται από τρίτο που έχει τέτοια εξουσία να αποκαλύψει δεδομένα[xxiii].

Ο ΓΚΠΔ έχει καταργήσει το δεύτερο κριτήριο, δηλαδή καταστάσεις στις οποίες η άσκηση δημόσιας εξουσίας είναι μέρος ενός προσώπου στο οποίο αποκαλύπτονται τα δεδομένα, δεν είναι πλέον σχετική βάση για την επεξεργασία δεδομένωνxxiv. Με άλλα λόγια, οι περιστάσεις υπό τις οποίες ο υπεύθυνος της ελεγκτικής υπηρεσίας μπορεί να επικαλεστεί αυτόν τον νομικό λόγο είναι πιο περιορισμένες από πριν.

Η δημόσια εξουσία ή η δημόσια αποστολή θα πρέπει κανονικά να αποδίδεται σε νόμους ή άλλους νομικούς κανονισμούς. Το WP29 έχει αναγνωρίσει ρητά ότι μετά τον ΓΚΠΔ, αυτό το νομικό υπόβαθρο πρέπει να ερμηνευθεί κατά τρόπο που να επιτρέπει στις δημόσιες αρχές κάποιο βαθμό ευελιξίας για την εξασφάλιση της ορθής διαχείρισης και λειτουργίας τους. Συνεπώς, οι δραστηριότητες αυτές δεν πρέπει να εμπίπτουν στο πεδίο εφαρμογής αυτού του νομικού πλαισίου και η επεξεργασία δεδομένων προσωπικού χαρακτήρα θα μπορούσε να βασίζεται στο νόμιμο συμφέρον[xxv].

Τελευταίο αλλά εξίσου σημαντικό, θα πρέπει να σημειωθεί ότι τα πρόσωπα στα οποία αναφέρονται τα δεδομένα έχουν το δικαίωμα να αντιταχθούν στην επεξεργασία βάσει αυτού του νομικού πλαισίου. Είναι ο ελεγκτής που έχει το βάρος να αποδείξει ότι έχει επιτακτικούς θεμιτούς λόγους για την επεξεργασία των προσωπικών δεδομένων[xxvi].

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

2.5.2. Εφαρμογή στο πλαίσιο της δραστηριότητας των Τοπικών Αρχών

Μεταξύ των νομικών υποχρεώσεων που απορρέουν από το άρθρο. 6, παράγραφος 1, στοιχείο «γ» του ΓΚΠΔ, η αποστολή που εκτελέστηκε για το δημόσιο συμφέρον / άσκηση δημόσιας εξουσίας θα ήταν ένας από τους σημαντικότερους νομικούς λόγους για τις δραστηριότητες των Τοπικών Αρχών. Παραδείγματα του WP29 για την εφαρμογή αυτού του λόγου περιλαμβάνουν τα εξής:

- μια φορολογική αρχή που συλλέγει και επεξεργάζεται την φορολογική δήλωση ενός ατόμου προκειμένου να καθορίσει και να επαληθεύσει το ποσό του φόρου που πρέπει να καταβληθεί - κατ 'αναλογία, αυτός ο λόγος θα μπορούσε να εφαρμοστεί και για τις αρχές τοπικής αυτοδιοίκησης που διαχειρίζονται τοπικούς φόρουςa;
- Ένα τοπικό κυβερνητικό σώμα (π.χ. δημοτική αρχή) που είναι έχει αναλάβει να λειτουργήσει μια υπηρεσία βιβλιοθήκης, ένα σχολείο ή τοπική πισίνα.

2.6. Νομικά Συμφέροντα

2.6.1. Σημασία & νομικές απαιτήσεις

Ο νομικός όρος «νόμιμα συμφέροντα» περιλαμβάνει δύο στοιχεία:

(i) Δικαιολογημένο συμφέρον του υπεύθυνου επεξεργασίας δεδομένων / τρίτων:

a. Η έννοια του «συμφέροντος» ορίζεται από το WP29 ως ένα ευρύτερο ποσοστό που μπορεί να έχει ο υπεύθυνος επεξεργασίας κατά την επεξεργασία ή το όφελος που μπορεί να αντλήσει ο ίδιος - ή η κοινωνία - από την επεξεργασία[xxvii]. Το συμφέρον μπορεί να ωφελήσει την κοινωνία εν γένει, αλλά μπορεί επίσης να είναι ευεργετικό μόνο για τον αντίστοιχο υπεύθυνο επεξεργασίας δεδομένων / τρίτο μέλος.

b. Η έννοια της «νομιμότητας» συνδέεται εγγενώς με τη συμμόρφωση με τη νομοθεσία - τόσο για το δίκαιο προστασίας των δεδομένων όσο και για τους νόμους που ισχύουν για την αντίστοιχη δραστηριότητα του υπεύθυνου επεξεργασίας. Με άλλα λόγια, οι τυχόν παράνομοι στόχοι που επιδιώκει ο υπεύθυνος επεξεργασίας / το τρίτο μέλος θα αποκλείσουν την εφαρμογή αυτού του νομικού πλαισίου. Το WP29 έχει κάνει μια μη- διεξοδική λίστα από τα συνηθέστερα σενάρια στα οποία θα μπορούσε να εφαρμοστεί το νόμιμο συμφέρον βάσει της παλαιάς οδηγίας 95/46. Οι περιοχές διαφέρουν λόγω διαφημιστικών/κερδοφορικών λόγων, (π.χ. άμεσο μάρκετινγκ, διαφήμιση ή ανεπιθύμητα μη εμπορικά μηνύματα, συμπεριλαμβανομένων των πολιτικών εκστρατειών ή της φιλανθρωπικής συγκέντρωσης κεφαλαίων) σε κοινωνικά ευεργετικές δραστηριότητες (π.χ. συστήματα

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

υποκλοπής, άσκηση του δικαιώματος στην ελευθερία έκφρασης ή ενημέρωσης ή πρόληψη της απάτης, κατάχρηση υπηρεσιών ή νομιμοποίηση εσόδων από παράνομες δραστηριότητες).

(ii) Το έννομο συμφέρον πρέπει να υπερισχύει των συμφερόντων, των θεμελιωδών δικαιωμάτων και των ελευθεριών και το υποκείμενο των δεδομένων = μια δοκιμή εξισορρόπησης θα πρέπει να εφαρμόζεται κατά περίπτωση. Η απαίτηση αυτή συνδέεται εγγενώς με την αρχή της αναλογικότητας. Παρόλο που ο υπεύθυνος επεξεργασίας δεδομένων / τρίτο μέλος μπορεί να έχει έννομο συμφέρον να διεξάγει τη διεκπεραίωση, αυτό μπορεί να είναι δυσανάλογο (π.χ. η αντίστοιχη επεξεργασία μπορεί να είναι πολύ παρεμβατική, σε υπερβολικά μεγάλη κλίμακα, χωρίς κατάλληλους περιορισμούς και διασφαλίσεις κ.λπ.) και σε ένα τέτοιο σενάριο η επεξεργασία δεν θα δικαιολογείται ως νόμιμη. Το WP29 έχει δηλώσει ότι μεταξύ των παραγόντων που απαιτούνται για τη διεξαγωγή της δοκιμής εξισορρόπησης είναι:

a. αξιολόγηση του νόμιμου συμφέροντος του υπευθύνου της επεξεργασίας ·
b. επίπτωση στα πρόσωπα στα οποία αναφέρονται τα δεδομένα ·
c. προσωρινό υπόλοιπο και
d. πρόσθετες διασφαλίσεις που εφαρμόζονται από τον υπεύθυνο επεξεργασίας για την αποτροπή τυχόν αδικαιολόγητων επιπτώσεων στα πρόσωπα στα οποία αναφέρονται τα δεδομένα [xxviii].

2.6.2. Εφαρμογή στο πλαίσιο της δραστηριότητας των Τοπικών Αρχών

Ο ΓΚΠΔ περιορίζει σημαντικά τη δυνατότητα εφαρμογής του νόμιμου συμφέροντος στο πλαίσιο των δραστηριοτήτων των δημόσιων αρχών. Προβλέπει ρητά ότι αυτός ο νομικός λόγος δεν εφαρμόζεται στην επεξεργασία που πραγματοποιείται από δημόσιες αρχές κατά την εκτέλεση των καθηκόντων τους. Το σκεπτικό πίσω από αυτή τη διάταξη είναι ότι οι δημόσιες αρχές πρέπει να έχουν τη νόμιμη εξουσιοδότηση να εκτελούν τα καθήκοντά τους.

Συνεπώς, οι Τοπικές Αρχές πρέπει να βασίζονται στο έννομο συμφέρον για την εκτέλεση των καθηκόντων τους, προκειμένου να επανεξετάσουν ποια άλλη νομική βάση για την επεξεργασία προσωπικών δεδομένων θα μπορούσαν να εφαρμόσουν (π.χ. καθήκον δημοσίου συμφέροντος / δημόσια αρχή).

Ωστόσο, το νόμιμο συμφέρον θα μπορούσε ακόμη να εφαρμοστεί από τις Τοπικές Αρχές ως έγκυρη νομική βάση για τις εσωτερικές διεργασίες τους - π.χ. στις δραστηριότητες Ανθρώπινου Δυναμικού.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

3. ΣΥΜΠΕΡΑΣΜΑ & ΠΡΑΚΤΙΚΕΣ ΣΥΜΒΟΥΛΕΣ

Η ικανότητα να προσδιοριστεί ποιος νομικός λόγος είναι εφαρμοστέος για τον οποίο η δραστηριότητα επεξεργασίας είναι απαραίτητη, είναι ουσιώδους σημασίας για κάθε υπεύθυνο επεξεργασίας δεδομένων προκειμένου να διασφαλιστεί η νομιμότητα της επεξεργασίας. Επιπλέον, οι πληροφορίες που ισχύουν για τον σκοπό της επεξεργασίας είναι ένα από τα βασικά στοιχεία της αρχής της διαφάνειας, δεδομένου ότι περιλαμβάνεται ρητά μεταξύ των πληροφοριών που πρέπει να παρέχονται σε κάθε υποκείμενο των δεδομένων από τον υπεύθυνο επεξεργασίας (άρθρο 13 και άρθρο 14 του ΓΚΠΔ). Ως εκ τούτου, τόσο οι δημόσιοι όσο και οι ιδιωτικοί υπεύθυνοι επεξεργασίας δεδομένων πρέπει να γνωρίζουν καλά την έννοια καθενός από τους νομικούς λόγους που απαριθμούνται στο άρθρο. 6 του ΓΚΠΔ. Ο κανονισμός δεν προβλέπει νέους νομικούς λόγους, αλλά τροποποιεί τις απαιτήσεις και τους όρους εφαρμογής για ορισμένους από τους υφιστάμενους (π.χ. συγκατάθεση, νόμιμα συμφέροντα). Σε κάθε περίπτωση, η δυνατότητα να προσδιοριστεί ο σωστός νομικός λόγος είναι το πρώτο βήμα για την εξασφάλιση της συμμόρφωσης με τον ΓΚΠΔ εντός του οργανισμού. Στο δόγμα αυτό υποδεικνύεται ότι ένας συνετός υπεύθυνος επεξεργασίας δεδομένων θα πρέπει να λάβει τα αναγκαία μέτρα για να εξασφαλίσει ότι σε περιπτώσεις όπου οι εποπτικές αρχές απαιτούν αποδείξεις, ο ελεγκτής θα πρέπει να μπορεί να επισημαίνει σε ποια κριτήρια στηρίζεται για την επεξεργασία και την κατάλληλη κοινοποίησή της στα υποκείμενα των δεδομένων[xxix].

4. ΕΞΩΤΕΡΙΚΕΣ ΠΗΓΕΣ & ΔΙΑΔΙΚΤΥΑΚΟΙ ΣΥΝΔΕΣΜΟΙ

Βιβλία

- **Voigt, P., von dem Bussche, A.**, The EU General Data Protection Regulation (GDPR) – A Practical Guide, Springer International Publishing (2017);
- **Boardman, R., Mullock, J., Mole, A.** Bird & Bird Guide to General Data Protection Regulation (2016);
- **EU** General Data Protection Regulation (GDPR). An Implementation and Compliance Guide, IT Governance Publishing, Cambridgeshire (2016);
- **European** Data Protection. Law and Practice, Executive Editor: Edurado Ustaran, CIPP/E, Partner, Hogan Lovells, IAPP (2018);

Έγγραφα της ομάδας εργασίας του άρθρου 29

- WP29, Guidelines on Consent under Regulation 2016/679, WP 259;

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

- WP29, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, WP 217;

Διαδικτυακοί Σύνδεσμοι

- http://europa.eu/rapid/press-release_IP-18-386_en.htm
- https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en
- https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/grounds-processing/when-can-personal-data-be-processed_en
- https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/grounds-processing/what-does-grounds-legitimate-interest-mean_en
- https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/grounds-processing/when-consent-valid_en
- https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/grounds-processing/does-consent-given-25-may-2018-continue-be-valid-once-gdpr-starts-apply-25-may-2018_en
- https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/grounds-processing/what-if-somebody-withdraws-their-consent_en
- https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/grounds-processing/what-if-somebody-withdraws-their-consent_en

5. ΠΑΡΑΠΟΜΠΕΣ

[i] WP29, Guidelines on Consent under Regulation 2016/679, WP 259, p. 6.
[ii] WP29, Guidelines on Consent under Regulation 2016/679, WP 259, p. 11-12.
[iii] More information on profiling is available in WP29 Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (project).
[iv] WP29, Guidelines on Consent under Regulation 2016/679, WP 259, p. 13.
[v] EU General Data Protection Regulation (GDPR). An Implementation and Compliance Guide, IT Governance Publishing, Cambridgeshire (2016), p. 189-190.
[vi] WP29, Guidelines on Consent under Regulation 2016/679, WP 259, p. 7.
[vii] The example is given in WP29, Guidelines on Consent under Regulation 2016/679, WP 259, p. 7.
[viii] WP29 Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, WP 217, p. 16-17.
[ix] Ibid, p. 16.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

[x] Voigt, P., von dem Bussche, A., The EU General Data Protection Regulation (GDPR) – A Practical Guide, Springer International Publishing (2017), p. 102.
[xi] European Data Protection. Law and Practice, Executive Editor: Edurado Ustaran, CIPP/E, Partner, Hogan Lovells, IAPP (2018), p. 118
[xii] WP29 Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, WP 217, p. 16.
[xiii] Ibid, p. 20.
[xiv] Boardman, R., Mullock, J., Mole, A. Bird & Bird Guide to General Data Protection Regulation (2016), p. 10.
[xv] WP29 Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, WP 217, p. 19.
[xvi] Ibid, p. 19.
[xvii] Ibid, p. 20.
[xviii] Ibid, p. 19.
[xix] Ibid, p. 20.
[xx] European Data Protection. Law and Practice, Executive Editor: Edurado Ustaran, CIPP/E, Partner, Hogan Lovells, IAPP (2018), p. 119.
[xxi] WP29 Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, WP 217, p. 20-21.
[xxii] Ibid, p. 21.
[xxiii] Ibid, p. 21.
[xxiv] European Data Protection. Law and Practice, Executive Editor: Edurado Ustaran, CIPP/E, Partner, Hogan Lovells, IAPP (2018), p. 119.
[xxv] WP29 Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, WP 217, p. 23.
[xxvi] European Data Protection. Law and Practice, Executive Editor: Edurado Ustaran, CIPP/E, Partner, Hogan Lovells, IAPP (2018), p. 119.
[xxvii] WP29 Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, WP 217, p. 24.
[xxviii] Ibid, p. 33.
[xxix] European Data Protection. Law and Practice, Executive Editor: Edurado Ustaran, CIPP/E, Partner, Hogan Lovells, IAPP (2018), p. 122.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

ProLegis

Επεξεργασία Ειδικών Κατηγοριών Προσωπικών Δεδομένων

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

ProLegis

Contents

1. ΝΟΜΙΚΟ ΠΛΑΙΣΙΟ 4

1.1. Χάρτης Θεμελιωδών Δικαιωμάτων της ΕΕ 4

1.2. ΓΚΠΔ 4

2. ΕΙΔΙΚΕΣ ΚΑΤΗΓΟΡΙΕΣ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ ΣΤΟ ΠΛΑΙΣΙΟ ΤΟΥ ΓΚΠΔ 11

2.1. Η λογική πίσω από τον ορισμό συγκεκριμένων κατηγοριών προσωπικών δεδομένων ως ειδικών 11

2.2. Είδη ειδικών κατηγοριών προσωπικών δεδομένων 12

2.3. Προσωπικά δεδομένα σχετικά με ποινικές καταδίκες και αξιόποινες πράξεις .. 14

3. ΝΟΜΙΚΟΙ ΛΟΓΟΙ ΓΙΑ ΤΗΝ ΕΠΕΞΕΡΓΑΣΙΑ ΕΙΔΙΚΩΝ ΚΑΤΗΓΟΡΙΩΝ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ 15

3.1. Ρητή συναίνεση 15

3.2. Υποχρεώσεις / ειδικά δικαιώματα στον τομέα της απασχόλησης, της κοινωνικής ασφάλισης και της νομοθεσίας κοινωνικής προστασίας 15

3.3. Ζωτικά συμφέροντα του υποκειμένου των δεδομένων ή άλλου φυσικού προσώπου 16

3.4. Επεξεργασία από μη κερδοσκοπικό σώμα με πολιτικό, φιλοσοφικό, θρησκευτικό ή συνδικαλιστικό σκοπό 17

3.5. Τα δεδομένα δημοσιοποιούνται εμφανώς από το υποκείμενο των δεδομένων 17

3.6. Ίδρυση, άσκηση ή υπεράσπιση νομικών αξιώσεων / δικαστηρίων που ενεργούν υπό την νομική τους ιδιότητα 18

3.7. Ουσιώδες δημόσιο συμφέρον βάσει του δικαίου της ΕΕ ή των κρατών μελών 18

3.8. Προληπτική ή επαγγελματική ιατρική, εκτίμηση της εργασιακής ικανότητας του εργαζομένου, ιατρική διάγνωση, παροχή υγειονομικής ή κοινωνικής φροντίδας ή θεραπείας 19

3.9. Το δημόσιο συμφέρον στον τομέα της δημόσιας υγείας 19

3.10. Επεξεργασία για αρχειοθετικούς σκοπούς γενικού συμφέροντος, επιστημονικούς ή ιστορικούς σκοπούς ή στατιστικούς σκοπούς 20

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

3.11. Περαιτέρω προϋποθέσεις στο δίκαιο των κρατών μελών 20
4. ΣΥΜΠΕΡΑΣΜΑ ΚΑΙ ΠΡΑΚΤΙΚΕΣ ΣΥΜΒΟΥΛΕΣ 20
5. ΕΞΩΤΕΡΙΚΕΣ ΠΗΓΕΣ & ΔΙΑΔΙΚΤΥΑΚΟΙ ΣΥΝΔΕΣΜΟΙ 21
Βιβλία 21
Έγγραφα της ομάδας εργασίας του άρθρου 29 21
Διαδικτυακοί Σύνδεσμοι 21
6. ΠΑΡΑΠΟΜΠΕΣ 21

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

1. ΝΟΜΙΚΟ ΠΛΑΙΣΙΟ

1.1. Χάρτης Θεμελιωδών Δικαιωμάτων της ΕΕ

Άρθρο 8

Προστασία των δεδομένων προσωπικού χαρακτήρα

1. Κάθε πρόσωπο έχει δικαίωμα στην προστασία των δεδομένων προσωπικού χαρακτήρα που το αφορούν.

2. Η επεξεργασία αυτών των δεδομένων πρέπει να γίνεται νομίμως, για καθορισμένους σκοπούς και με βάση τη συγκατάθεση του ενδιαφερομένου ή για άλλους θεμιτούς λόγους που προβλέπονται από το νόμο. Κάθε πρόσωπο δικαιούται να έχει πρόσβαση στα συλλεγέντα δεδομένα που το αφορούν και να επιτυγχάνει τη διόρθωσή τους.

3. Ο σεβασμός των κανόνων αυτών υπόκειται στον έλεγχο ανεξάρτητης αρχής.

1.2. ΓΚΠΔ

Αιτιολογική Σκέψη (51)

Δεδομένα προσωπικού χαρακτήρα τα οποία είναι εκ φύσεως ιδιαίτερα ευαίσθητα σε σχέση με θεμελιώδη δικαιώματα και ελευθερίες χρήζουν ειδικής προστασίας, καθότι το πλαίσιο της επεξεργασίας τους θα μπορούσε να δημιουργήσει σημαντικούς κινδύνους για τα θεμελιώδη δικαιώματα και τις ελευθερίες. Τα εν λόγω δεδομένα προσωπικού χαρακτήρα θα πρέπει να περιλαμβάνουν δεδομένα προσωπικού χαρακτήρα που αποκαλύπτουν φυλετική ή εθνοτική καταγωγή, όπου η χρήση του όρου «φυλετική καταγωγή» στον παρόντα κανονισμό δεν συνεπάγεται ότι η Ένωση αποδέχεται θεωρίες που υποστηρίζουν την ύπαρξη χωριστών ανθρώπινων φυλών. Η επεξεργασία φωτογραφιών δεν θα πρέπει συστηματικά να θεωρείται ότι είναι επεξεργασία ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα, καθώς αυτές καλύπτονται από τον ορισμό των βιομετρικών δεδομένων μόνο σε περίπτωση επεξεργασίας μέσω ειδικών τεχνικών μέσων που επιτρέπουν την αδιαμφισβήτητη ταυτοποίηση ή επαλήθευση της ταυτότητας ενός φυσικού προσώπου. Τέτοια δεδομένα προσωπικού χαρακτήρα δεν θα πρέπει να υποβάλλονται σε επεξεργασία, εκτός εάν η επεξεργασία επιτρέπεται σε ειδικές περιπτώσεις που προβλέπονται στον παρόντα κανονισμό, λαμβάνοντας υπόψη ότι το δίκαιο των κρατών μελών μπορεί να προβλέπει ειδικές διατάξεις για την προστασία των δεδομένων, προκειμένου να προσαρμόζεται η εφαρμογή των κανόνων του παρόντος κανονισμού

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

λόγω συμμόρφωσης προς νομική υποχρέωση ή λόγω εκπλήρωσης καθήκοντος που εκτελείται προς το δημόσιο συμφέρον ή κατά την άσκηση δημόσιας εξουσίας που έχει ανατεθεί στον υπεύθυνο επεξεργασίας. Εκτός από τις ειδικές απαιτήσεις στις οποίες υπάγεται η εν λόγω επεξεργασία, θα πρέπει να εφαρμόζονται οι γενικές αρχές και οι λοιποί κανόνες του παρόντος κανονισμού, ιδίως σε ό,τι αφορά τους όρους νόμιμης επεξεργασίας. Παρεκκλίσεις από τη γενική απαγόρευση επεξεργασίας δεδομένων προσωπικού χαρακτήρα που υπάγονται στις εν λόγω ειδικές κατηγορίες θα πρέπει να προβλέπονται ρητώς, μεταξύ άλλων, σε περίπτωση ρητής συγκατάθεσης του υποκειμένου των δεδομένων ή όταν πρόκειται για ειδικές ανάγκες, ιδίως όταν η επεξεργασία διενεργείται στο πλαίσιο θεμιτών δραστηριοτήτων ορισμένων ενώσεων ή ιδρυμάτων, σκοπός των οποίων είναι να επιτρέπουν την άσκηση των θεμελιωδών ελευθεριών.

Αιτιολογική Σκέψη (52)

Η παρέκκλιση από την απαγόρευση επεξεργασίας ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα θα πρέπει να επιτρέπεται επίσης όταν προβλέπεται από το δίκαιο της Ένωσης ή κράτους μέλους και με την επιφύλαξη κατάλληλων εγγυήσεων, ώστε να προστατεύονται τα δεδομένα προσωπικού χαρακτήρα και άλλα θεμελιώδη δικαιώματα, εφόσον δικαιολογείται από λόγους δημόσιου συμφέροντος, ιδίως η επεξεργασία δεδομένων προσωπικού χαρακτήρα στον τομέα του εργατικού δικαίου, του δικαίου κοινωνικής προστασίας, συμπεριλαμβανομένων των συντάξεων, και για σκοπούς υγειονομικής ασφάλειας, παρακολούθησης και συναγερμού και για την πρόληψη ή τον έλεγχο των μεταδοτικών ασθενειών και άλλων σοβαρών απειλών κατά της υγείας. Αυτή η παρέκκλιση μπορεί να γίνεται για υγειονομικούς σκοπούς, συμπεριλαμβανομένων της δημόσιας υγείας και της διαχείρισης υπηρεσιών υγειονομικής περίθαλψης, προκειμένου ειδικότερα να διασφαλίζονται η ποιότητα και η αποδοτικότητα ως προς το κόστος των διαδικασιών που χρησιμοποιούνται για τον διακανονισμό αξιώσεων για παροχές και υπηρεσίες στο σύστημα υγειονομικής ασφάλισης, ή για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον, σκοπούς επιστημονικής ή ιστορικής έρευνας ή στατιστικούς σκοπούς. Θα πρέπει επίσης να προβλεφθεί παρέκκλιση που να επιτρέπει την επεξεργασία τέτοιων δεδομένων προσωπικού χαρακτήρα όταν είναι αναγκαία για τη θεμελίωση, άσκηση ή υποστήριξη νομικών αξιώσεων, είτε σε δικαστική διαδικασία είτε σε διοικητική ή τυχόν εξωδικαστική διαδικασία.

Αιτιολογική Σκέψη (53)

Η επεξεργασία ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα που χρήζουν υψηλότερης προστασίας θα πρέπει να γίνεται μόνο για σκοπούς που σχετίζονται με την υγεία, εφόσον αυτό είναι απαραίτητο για την επίτευξη των εν λόγω στόχων, προς όφελος

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

των φυσικών προσώπων και της κοινωνίας στο σύνολό της, ιδίως στο πλαίσιο της διαχείρισης των υπηρεσιών και συστημάτων υγειονομικής περίθαλψης και κοινωνικής μέριμνας, μεταξύ άλλων και της επεξεργασίας των δεδομένων αυτών από τις διαχειριστικές και τις κεντρικές εθνικές υγειονομικές αρχές για τον σκοπό του ποιοτικού ελέγχου, της διαχείρισης των πληροφοριών και της συνολικής εθνικής και τοπικής εποπτείας του συστήματος υγείας ή κοινωνικής μέριμνας, και της εξασφάλισης της συνέχειας της υγειονομικής περίθαλψης ή κοινωνικής μέριμνας και της διασυνοριακής υγειονομικής περίθαλψης ή της υγειονομικής ασφάλειας, για σκοπούς παρακολούθησης και συναγερμού ή για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον, για σκοπούς επιστημονικής ή ιστορικής έρευνας ή στατιστικούς σκοπούς, βάσει του δικαίου της Ένωσης ή των κρατών μελών και με απώτερο στόχο την εξυπηρέτηση του δημόσιου συμφέροντος, καθώς και για μελέτες που διενεργούνται προς το δημόσιο συμφέρον στον τομέα της δημόσιας υγείας. Συνεπώς, ο παρών κανονισμός θα πρέπει να προβλέπει εναρμονισμένες προϋποθέσεις για την επεξεργασία των ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα που αφορούν την υγεία, σε σχέση με ειδικές ανάγκες, ιδίως όταν η επεξεργασία των εν λόγω δεδομένων πραγματοποιείται για ορισμένους σκοπούς που αφορούν την υγεία από πρόσωπα που υπέχουν νομική υποχρέωση τήρησης επαγγελματικού απορρήτου. Το δίκαιο της Ένωσης ή των κρατών μελών θα πρέπει να προβλέπει ειδικά και κατάλληλα μέτρα για την προστασία των θεμελιωδών δικαιωμάτων και των δεδομένων προσωπικού χαρακτήρα των φυσικών προσώπων. Τα κράτη μέλη θα πρέπει να μπορούν να διατηρούν ή να θεσπίζουν περαιτέρω όρους, μεταξύ άλλων και περιορισμούς, όσον αφορά την επεξεργασία γενετικών δεδομένων, βιομετρικών δεδομένων ή δεδομένων που αφορούν την υγεία. Ωστόσο, αυτό δεν θα πρέπει να εμποδίζει την ελεύθερη κυκλοφορία δεδομένων προσωπικού χαρακτήρα εντός της Ένωσης, όταν οι όροι αυτοί εφαρμόζονται στη διασυνοριακή επεξεργασία των δεδομένων αυτών.

Αιτιολογική Σκέψη (54)

Η επεξεργασία ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα μπορεί να είναι απαραίτητη για λόγους δημόσιου συμφέροντος στους τομείς της δημόσιας υγείας, χωρίς τη συναίνεση του υποκειμένου των δεδομένων. Η εν λόγω επεξεργασία θα πρέπει να υπόκειται σε κατάλληλα και ειδικά μέτρα για την προστασία των δικαιωμάτων και ελευθεριών των φυσικών προσώπων. Στο πλαίσιο αυτό, η «δημόσια υγεία» θα πρέπει να ερμηνεύεται όπως ορίζεται στον κανονισμό (ΕΚ) αριθ. 1338/2008 του Ευρωπαϊκού Κοινοβουλίου και του Συμβουλίου (1), δηλαδή ως το σύνολο των στοιχείων που συνδέονται με την υγεία, συγκεκριμένα η κατάσταση της υγείας, περιλαμβανομένων της νοσηρότητας και αναπηρίας, οι καθοριστικοί παράγοντες που επιδρούν στην κατάσταση της υγείας, οι ανάγκες υγειονομικής περίθαλψης, οι πόροι που διατίθενται για την

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

υγειονομική περίθαλψη, η παροχή υγειονομικής περίθαλψης και η πρόσβαση από όλους σε αυτήν, καθώς και οι δαπάνες και η χρηματοδότηση της υγειονομικής περίθαλψης και οι αιτίες θνησιμότητας. Αυτή η επεξεργασία δεδομένων σχετικών με την υγεία για λόγους δημόσιου συμφέροντος δεν θα πρέπει να έχει ως αποτέλεσμα την επεξεργασία δεδομένων προσωπικού χαρακτήρα για άλλους σκοπούς από τρίτους, όπως εργοδότες ή ασφαλιστικέςεταιρείες και τράπεζες.

Αιτιολογική Σκέψη (55)

Επιπλέον, η επεξεργασία δεδομένων προσωπικού χαρακτήρα από δημόσιες αρχές με σκοπό την επίτευξη σκοπών επίσημα αναγνωρισμένων θρησκευτικών ενώσεων, οι οποίοι προβλέπονται στο συνταγματικό ή το διεθνές δημόσιο δίκαιο, πραγματοποιείται για λόγους δημόσιου συμφέροντος.

Αιτιολογική Σκέψη (56)

Εάν, στο πλαίσιο εκλογικών δραστηριοτήτων, η λειτουργία του δημοκρατικού συστήματος σε ένα κράτος μέλος απαιτεί τη συγκέντρωση από τα πολιτικά κόμματα δεδομένων προσωπικού χαρακτήρα σχετικά με τα πολιτικά φρονήματα των πολιτών, η επεξεργασία των εν λόγω δεδομένων μπορεί να επιτρέπεται για λόγους δημόσιου συμφέροντος, εφόσον προβλέπονται κατάλληλες εγγυήσεις.

Άρθρο 4

Ορισμοί

Για τους σκοπούς του παρόντος κανονισμού νοούνται ως:

[…]

*(13) «**γενετικά δεδομένα**»: τα δεδομένα προσωπικού χαρακτήρα που αφορούν τα γενετικά χαρακτηριστικά φυσικού προσώπου που κληρονομήθηκαν ή αποκτήθηκαν, όπως προκύπτουν, ιδίως, από ανάλυση βιολογικού δείγματος του εν λόγω φυσικού προσώπου και τα οποία παρέχουν μοναδικές πληροφορίες σχετικά με την φυσιολογία ή την υγεία του εν λόγω φυσικού προσώπου,*

*(14) «**βιομετρικά δεδομένα**»: δεδομένα προσωπικού χαρακτήρα τα οποία προκύπτουν από ειδική τεχνική επεξεργασία συνδεόμενη με φυσικά, βιολογικά ή συμπεριφορικά χαρακτηριστικά φυσικού προσώπου και τα οποία επιτρέπουν ή*

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

επιβεβαιώνουν την αδιαμφισβήτητη ταυτοποίηση του εν λόγω φυσικού προσώπου, όπως εικόνες προσώπου ή δακτυλοσκοπικά δεδομένα,

*(15) «**δεδομένα που αφορούν την υγεία**»: δεδομένα προσωπικού χαρακτήρα τα οποία σχετίζονται με τη σωματική ή ψυχική υγεία ενός φυσικού προσώπου, περιλαμβανομένης της παροχής υπηρεσιών υγειονομικής φροντίδας, και τα οποία αποκαλύπτουν πληροφορίες σχετικά με την κατάσταση της υγείας του,*

Άρθρο 9

Επεξεργασία ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα

1. **Απαγορεύεται η επεξεργασία δεδομένων προσωπικού χαρακτήρα που αποκαλύπτουν τη φυλετική ή εθνοτική καταγωγή, τα πολιτικά φρονήματα, τις θρησκευτικές ή φιλοσοφικές πεποιθήσεις ή τη συμμετοχή σε συνδικαλιστική οργάνωση, καθώς και η επεξεργασία γενετικών δεδομένων, βιομετρικών δεδομένων με σκοπό την αδιαμφισβήτητη ταυτοποίηση προσώπου, δεδομένων που αφορούν την υγεία ή δεδομένων που αφορούν τη σεξουαλική ζωή φυσικού προσώπου ή τον γενετήσιο προσανατολισμό.**

2. **Η παράγραφος 1 δεν εφαρμόζεται** στις ακόλουθες περιπτώσεις:

(α) το υποκείμενο των δεδομένων έχει παράσχει ρητή συγκατάθεση για την επεξεργασία αυτών των δεδομένων προσωπικού χαρακτήρα για έναν ή περισσότερους συγκεκριμένους σκοπούς, εκτός εάν το δίκαιο της Ένωσης ή κράτους μέλους προβλέπει ότι η απαγόρευση που αναφέρεται στην παράγραφο 1 δεν μπορεί να αρθεί από το υποκείμενο των δεδομένων,

(β) η επεξεργασία είναι απαραίτητη για την εκτέλεση των υποχρεώσεων και την άσκηση συγκεκριμένων δικαιωμάτων του υπευθύνου επεξεργασίας ή του υποκειμένου των δεδομένων στον τομέα του εργατικού δικαίου και του δικαίου κοινωνικής ασφάλισης και κοινωνικής προστασίας, εφόσον επιτρέπεται από το δίκαιο της Ένωσης ή κράτους μέλους ή από συλλογική συμφωνία σύμφωνα με το εθνικό δίκαιο παρέχοντας κατάλληλες εγγυήσεις για τα θεμελιώδη δικαιώματα και τα συμφέροντα του υποκειμένου των δεδομένων,

(γ) η επεξεργασία είναι απαραίτητη για την προστασία των ζωτικών συμφερόντων του υποκειμένου των δεδομένων ή άλλου φυσικού προσώπου, εάν το υποκείμενο των δεδομένων είναι σωματικά ή νομικά ανίκανο να συγκατατεθεί,

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

(δ) η επεξεργασία διενεργείται, με κατάλληλες εγγυήσεις, στο πλαίσιο των νόμιμων δραστηριοτήτων ιδρύματος, οργάνωσης ή άλλου μη κερδοσκοπικού φορέα με πολιτικό, φιλοσοφικό, θρησκευτικό ή συνδικαλιστικό στόχο και υπό την προϋπόθεση ότι η επεξεργασία αφορά αποκλειστικά τα μέλη ή τα πρώην μέλη του φορέα ή πρόσωπα τα οποία έχουν τακτική επικοινωνία μαζί του σε σχέση με τους σκοπούς του και ότι τα δεδομένα προσωπικού χαρακτήρα δεν κοινοποιούνται εκτός του συγκεκριμένου φορέα χωρίς τη συγκατάθεση των υποκειμένων των δεδομένων,

(ε) η επεξεργασία αφορά δεδομένα προσωπικού χαρακτήρα τα οποία έχουν προδήλως δημοσιοποιηθεί από το υποκείμενο των δεδομένων,

(στ) η επεξεργασία είναι απαραίτητη για τη θεμελίωση, άσκηση ή υποστήριξη νομικών αξιώσεων ή όταν τα δικαστήρια ενεργούν υπό τη δικαιοδοτική τους ιδιότητα,

(ζ) η επεξεργασία είναι απαραίτητη για λόγους ουσιαστικού δημόσιου συμφέροντος, βάσει του δικαίου της Ένωσης ή κράτους μέλους, το οποίο είναι ανάλογο προς τον επιδιωκόμενο στόχο, σέβεται την ουσία του δικαιώματος στην προστασία των δεδομένων και προβλέπει κατάλληλα και συγκεκριμένα μέτρα για τη διασφάλιση των θεμελιωδών δικαιωμάτων και των συμφερόντων του υποκειμένου των δεδομένων,

(η) η επεξεργασία είναι απαραίτητη για σκοπούς προληπτικής ή επαγγελματικής ιατρικής, εκτίμησης της ικανότητας προς εργασία του εργαζομένου, ιατρικής διάγνωσης, παροχής υγειονομικής ή κοινωνικής περίθαλψης ή θεραπείας ή διαχείρισης υγειονομικών και κοινωνικών συστημάτων και υπηρεσιών βάσει του ενωσιακού δικαίου ή του δικαίου κράτους μέλους ή δυνάμει σύμβασης με επαγγελματία του τομέα της υγείας και με την επιφύλαξη των προϋποθέσεων και των εγγυήσεων που αναφέρονται στην παράγραφο 3,

(θ) η επεξεργασία είναι απαραίτητη για λόγους δημόσιου συμφέροντος στον τομέα της δημόσιας υγείας, όπως η προστασία έναντι σοβαρών διασυνοριακών απειλών κατά της υγείας ή η διασφάλιση υψηλών προτύπων ποιότητας και ασφάλειας της υγειονομικής περίθαλψης και των φαρμάκων ή των ιατροτεχνολογικών προϊόντων, βάσει του δικαίου της Ένωσης ή του δικαίου κράτους μέλους, το οποίο προβλέπει κατάλληλα και συγκεκριμένα μέτρα για την προστασία των δικαιωμάτων και ελευθεριών του υποκειμένου των δεδομένων, ειδικότερα δε του επαγγελματικού απορρήτου, ή L 119/38 EL Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης 4.5.2016

(ι) η επεξεργασία είναι απαραίτητη για σκοπούς αρχειοθέτησης προς το δημόσιο συμφέρον, για σκοπούς επιστημονικής ή ιστορικής έρευνας ή για στατιστικούς σκοπούς σύμφωνα με το άρθρο 89 παράγραφος 1 βάσει του δικαίουτης Ένωσης ή κράτους

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

μέλους, οι οποίοι είναι ανάλογοι προς τον επιδιωκόμενο στόχο, σέβονται την ουσία του δικαιώματος στην προστασία των δεδομένων και προβλέπουν κατάλληλα και συγκεκριμένα μέτρα για τη διασφάλιση των θεμελιωδών δικαιωμάτων και των συμφερόντων του υποκειμένου των δεδομένων.

3. Τα δεδομένα προσωπικού χαρακτήρα που αναφέρονται στην παράγραφο 1 μπορεί να τύχουν επεξεργασίας για τους σκοπούς που προβλέπονται στην παράγραφο 2 στοιχείο η), όταν τα δεδομένα αυτά υποβάλλονται σε επεξεργασία από ή υπό την ευθύνη επαγγελματία που υπόκειται στην υποχρέωση τήρησης του επαγγελματικού απορρήτου βάσει του δικαίου της Ένωσης ή κράτους μέλους ή βάσει κανόνων που θεσπίζονται από αρμόδιους εθνικούς φορείς ή από άλλο πρόσωπο το οποίο υπέχει επίσης υποχρέωση τήρησης του απορρήτου βάσει του δικαίου της Ένωσης ή κράτους μέλους ή βάσει κανόνων που θεσπίζονται από αρμόδιους εθνικούς φορείς.

4. Τα κράτη μέλη μπορούν να διατηρούν ή να θεσπίζουν περαιτέρω όρους, μεταξύ άλλων και περιορισμούς, όσον αφορά την επεξεργασία γενετικών δεδομένων, βιομετρικών δεδομένων ή δεδομένων που αφορούν την υγεία.

Άρθρο 10

Επεξεργασία δεδομένων προσωπικού χαρακτήρα που αφορούν ποινικές καταδίκες και αδικήματα

Η επεξεργασία δεδομένων προσωπικού χαρακτήρα που αφορούν ποινικές καταδίκες και αδικήματα ή σχετικά μέτρα ασφάλειας *που βασίζονται στο άρθρο 6 παράγραφος 1 διενεργείται* ***μόνο υπό τον έλεγχο επίσημης αρχής ή εάν η επεξεργασία επιτρέπεται από το δίκαιο της Ένωσης ή το δίκαιο κράτους μέλους*** *το οποίο προβλέπει επαρκείς εγγυήσεις για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων. Πλήρες ποινικό μητρώο τηρείται μόνο υπό τον έλεγχο επίσημης αρχής.*

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

2. ΕΙΔΙΚΕΣ ΚΑΤΗΓΟΡΙΕΣ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ ΣΤΟ ΠΛΑΙΣΙΟ ΤΟΥ ΓΚΠΔ

2.1. Η λογική πίσω από τον ορισμό συγκεκριμένων κατηγοριών προσωπικών δεδομένων ως ειδικών

Ακόμη και κατά την εκπόνηση της πρώτης νομοθετικής πράξης της ΕΕ για την προστασία των δεδομένων προσωπικού χαρακτήρα - Οδηγία 95/46 - η Ευρωπαϊκή Επιτροπή υπογράμμισε ότι η επεξεργασία ορισμένων κατηγοριών προσωπικών δεδομένων θα μπορούσε να συνεπάγεται υψηλότερο κίνδυνο για τα θεμελιώδη δικαιώματα και τις ελευθερίες των ευρωπαίων πολιτών[i]. Έτσι, θεσπίστηκε γενική απαγόρευση για την επεξεργασία τέτοιων «επικίνδυνων» κατηγοριών προσωπικών δεδομένων. Ονομάζονταν «ειδικές κατηγορίες προσωπικών δεδομένων», αλλά στην πράξη ονομάζονταν επίσης «ευαίσθητα δεδομένα» λόγω της ευαίσθητης φύσης τους για την ιδιωτική σφαίρα του ατόμου[ii]. Τα δεδομένα αυτά μπορούν να υποβάλλονται σε επεξεργασία μόνο σε εξαιρετικές περιπτώσεις, οι οποίες αναφέρονται αναλυτικά στη νομοθεσία περί προστασίας των δεδομένων των κρατών μελών.

Ο ΓΚΠΔ συνεχίζει την προσέγγιση αυτή, αλλά διευρύνει το πεδίο των ειδικών κατηγοριών προσωπικών δεδομένων και προβλέπει ορισμένες νέες εξαιρέσεις (νομικούς λόγους) που παρέχουν στους υπεύθυνους επεξεργασίας τη δυνατότητα επεξεργασίας τέτοιων δεδομένων.

Πρέπει να αναφερθεί ότι διάφοροι τύποι δεδομένων έχουν διαφορετικό αντίκτυπο των ατόμων. Το ποια δεδομένα ορίζονται ως ευαίσθητα βασίζονται σε μια αντικειμενική και όχι υποκειμενική αρχή. Με άλλα λόγια, κάποιος μπορεί να αισθάνεται ότι τα δεδομένα που σχετίζονται με την οικονομική του κατάσταση, το ιστορικό των πειθαρχικών κυρώσεων, τον Μοναδικό Αριθμό Αναγνώρισης ή τον Αριθμός Κοινωνικής Ασφάλισης είναι ευαίσθητα. Ωστόσο, εάν τα δεδομένα αυτά δεν αναγνωρίζονται από τον ευρωπαίο νομοθέτη ως ευαίσθητα, δεν εμπίπτουν στο ειδικό καθεστώς επεξεργασίας των δεδομένων αυτών, ανεξαρτήτως του ευαίσθητου του χαρακτήρα τους, από υποκειμενική άποψη.

Στο δόγμα, επισημαίνεται ότι η επιλογή για το ποιες κατηγορίες προσωπικών δεδομένων πρέπει να οριστούν ως ειδικές, επηρεάστηκε ουσιαστικά από τους νόμους κατά των διακρίσεων, γεγονός που εξηγεί γιατί δεδομένα, όπως οι Αριθμοί Κοινωνικής Ασφάλισης και τα στοιχεία της πιστωτικής κάρτας (τα οποία αν χρησιμοποιούνταν με λάθος τρόπο θα μπορούσαν να προκαλέσουν σοβαρή βλάβη στα άτομα) δεν ορίζονται ως ευαίσθητα[iii].

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

2.2. Είδη ειδικών κατηγοριών προσωπικών δεδομένων

Σύμφωνα με το άρθρο 9, παρ. 1 του ΓΚΠΔ, οι ακόλουθοι τύποι προσωπικών δεδομένων είναι ειδική κατηγορία (ευαίσθητα δεδομένα):

- **Προσωπικά δεδομένα που αποκαλύπτουν τη φυλετική ή εθνοτική καταγωγή** = αυτές οι κατηγορίες προσωπικών δεδομένων ορίζονται ως ευαίσθητες, όπως αυτές συνεπάγονται υψηλό κίνδυνο διακρίσεων. Στο νομικό δόγμα, δίνονται τα ακόλουθα παραδείγματα σχετικά με τα δεδομένα που θα μπορούσαν να εμπίπτουν στην κατηγορία αυτή: το όνομα και το επώνυμο του ατόμου, τον τόπο γέννησής του, τη μητρική του γλώσσα ή τα ονόματα των γονέων του που θα μπορούσαν, όταν συνδυάστηκαν, να επιτρέψουν συμπεράσματα ως προς την καταγωγή του [iv];
- **Πολιτικές απόψεις** = αυτά τα δεδομένα χρήζουν ιδιαίτερης προστασίας, επειδή σχετίζονται με την εγγύηση στους πολίτες να διαμορφώνουν απόψεις σχετικά με την πολιτική και τελικά να συμμετάσχουν (ενεργά ως πολιτικοί ή παθητικά ως εκλογείς και μέλη της κοινωνίας των πολιτών) στην πολιτική ζωή της χώρας. Παραδείγματα τέτοιων δεδομένων περιλαμβάνουν πληροφορίες σχετικά με τα μέλη ενός πολιτικού κόμματος, πληροφορίες σχετικά με την ένταξη σε οποιεσδήποτε αναφορές, συμμετοχή σε διαδηλώσεις, πολιτική επανένωση ή παρόμοια εκδήλωση, πληροφορίες σχετικά με την υποστήριξη μιας συγκεκριμένης πολιτικής ιδέας ή την απόρριψή της [v]
- **Θρησκευτικές ή φιλοσοφικές πεποιθήσεις** = αυτές οι κατηγορίες δεδομένων συνδέονται στενά με την ελευθερία της συνείδησης, δηλαδή την ελευθερία να αποφασίζουμε αν θα πιστεύουμε σε υπερβατικές δυνάμεις που προκαθορίζουν την καθημερινή ζωή μας και αν θα την εκδηλώσουμε ή όχι. Η ιστορία της ανθρωπότητας είναι γεμάτη από παραδείγματα όπου η βία έχει εκδηλωθεί στη βάση θρησκευτικών διαφορών, επομένως, τα δεδομένα αυτά πρέπει επίσης να είναι ειδικά προστατευμένα σύμφωνα με τους νόμους περί προστασίας των δεδομένων.
- **Μέλη συνδικαλιστικών οργανώσεων** = πληροφορίες που αφορούν αυτά τα μέλη είναι ευαίσθητες, διότι δημιουργούν τον κίνδυνο μεροληπτικής μεταχείρισης στον τομέα της εργατικής νομοθεσίας. Οι Ευρωπαίοι πολίτες έχουν την ελευθερία να διεξάγουν συλλογικές διαπραγματεύσεις και δράσεις, και επομένως δεν πρέπει να αντιμετωπίζονται άνισα βάσει της συνδικαλιστικής τους συνείδησης [vi];
- **Γενετικά δεδομένα** = νέα κατηγορία που εισήχθη από τον ΓΚΠΔ ως ευαίσθητη κατηγορία δεδομένων. Ο ΓΚΠΔ τα ορίζει ως «τα δεδομένα προσωπικού χαρακτήρα που αφορούν τα γενετικά χαρακτηριστικά φυσικού προσώπου που κληρονομήθηκαν ή αποκτήθηκαν, όπως προκύπτουν, ιδίως, από ανάλυση

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

βιολογικού δείγματος του εν λόγω φυσικού προσώπου και τα οποία παρέχουν μοναδικές πληροφορίες σχετικά με την φυσιολογία ή την υγεία του εν λόγω φυσικού προσώπου». Ορισμένα κράτη μέλη έχουν ήδη αναγνωρίσει το καθεστώς του ευαίσθητου αυτού του τύπου δεδομένων[vii], αλλά για πρώτη φορά ο ΓΚΠΔ το εισάγει σε επίπεδο ΕΕ. Τα γενετικά δεδομένα πρέπει να προστατεύονται, επειδή τέτοιοι τύποι δεδομένων αφορούν όχι μόνο το αντίστοιχο υποκείμενο των δεδομένων, αλλά θα μπορούσε επίσης να επηρεάσει τον απροσδιόριστο κύκλο των ατόμων που είναι μέρος της γενεαλογίας του ατόμου (συμπεριλαμβανομένων των δεδομένων του θανάτου, των δεδομένων των παιδιών κ.λπ.). Επιπλέον, η λεπτομερής ανάλυση τέτοιων δεδομένων θα μπορούσε να αποκαλύψει άλλους τύπους ευαίσθητων πληροφοριών, όπως ψυχολογικά ή υγειονομικά δεδομένα (π.χ., προδιάθεση για ασθένειες, ευπάθεια κ.λπ.) ·

- **Βιομετρικά δεδομένα με σκοπό τη μοναδική αναγνώριση ενός φυσικού προσώπου** = αυτοί οι τύποι δεδομένων χρήζουν προστασίας, διότι επιτρέπουν στους υπεύθυνους επεξεργασίας αδιαμφισβήτητα να προσδιορίζουν ένα συγκεκριμένο φυσικό πρόσωπο με βάση τα φυσικά ή συμπεριφορικά χαρακτηριστικά τους: (δακτυλικά αποτυπώματα, αναγνώριση προσώπου, ίριδας, αμφιβληστροειδούς, αγγειακά μοντέλα, DNA, ομιλία, υπογραφή, αλληλεπίδραση πληκτρολογίου κ.λπ.). Καθώς η επεξεργασία τέτοιων τύπων δεδομένων γίνεται ολοένα και πιο συνηθισμένη με την εισαγωγή διαφόρων τεχνολογικών αποφάσεων (π.χ. συστήματα ελέγχου πρόσβασης σε χώρους, συστήματα αναγνώρισης σε απομακρυσμένες συσκευές όπως κινητά τηλέφωνα, τάμπλετς κλπ.), η επεξεργασία αυτή πρέπει να είναι πιο περιορισμένη και ελεγχόμενη και αυτοί οι παράγοντες δικαιολογούν τη συμπερίληψη αυτών των δεδομένων στον κατάλογο των «ευαίσθητων» δεδομένων στον ΓΚΠΔ. Σε αντίθεση με τις πρακτικές που έχουν θεσπιστεί σε ορισμένα κράτη μέλη, η επεξεργασία των φωτογραφιών δεν θα θεωρείται αυτομάτως ως ευαίσθητη επεξεργασία. Οι φωτογραφίες θα θεωρούνται ευαίσθητα δεδομένα μόνο εάν επιτρέπουν τη μοναδική αναγνώριση ή πιστοποίηση ενός ατόμου ως βιομετρική (π.χ. σε ηλεκτρονικό διαβατήριο ή άλλο έγγραφο ταυτότητας)[viii];
- **Δεδομένα σχετικά με την υγεία ή τη σεξουαλική ζωή ή το σεξουαλικό προσανατολισμό ενός φυσικού προσώπου** = αυτά τα δεδομένα είναι πολύ ευαίσθητα, καθώς παρεμβαίνουν μέσα στις πιο στενές πτυχές της ζωής του ατόμου. Επιπλέον, οι πληροφορίες σχετικά με τη σεξουαλική ζωή και τον γενετήσιο προσανατολισμό συνεπάγονται τον κίνδυνο διακρίσεων, χειραγώγησης κ.λπ. Στη θεωρία αναφέρεται ότι αυτά τα δεδομένα περιλαμβάνουν επίσης την ακριβή ταυτότητα του/των συντόφου/ων του ατόμου [ix]

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

2.3. Προσωπικά δεδομένα σχετικά με ποινικές καταδίκες και αξιόποινες πράξεις

Τα προσωπικά δεδομένα που αφορούν ποινικές καταδίκες και αδικήματα ή συναφή μέτρα ασφαλείας δεν διακηρύσσονται ως ειδική κατηγορία προσωπικών δεδομένων. Ωστόσο, η νομοθεσία ορισμένων κρατών μελών τα αντιμετωπίζει ως ευαίσθητα[x]. Παρόλα αυτά, οι εν λόγω τύποι πληροφοριών συνεπάγονται επίσης τον κίνδυνο άνισης μεταχείρισης (π.χ. στον τομέα της απασχόλησης), συνεπώς, τα δεδομένα αυτά υπόκεινται επίσης σε ειδικούς κανόνες επεξεργασίας. Ο ΓΚΠΔ δεν εισάγει σημαντικές τροποποιήσεις σε σχέση με την παλαιά οδηγία 95/46 όσον αφορά τα δεδομένα ποινικών καταδίκων και αδικημάτων. Παράλληλα, δεδομένου ότι οι κανόνες της οδηγίας μεταφέρθηκαν με διαφορετικό τρόπο στο Κράτος Μέλος, ο ΓΚΠΔ θα καθιερώσει μια γενικότερη προσέγγιση σε επίπεδο ΕΕ σε σχέση με τα δεδομένα αυτά. Σύμφωνα με τη διατύπωση του άρθρου 10 του ΓΚΠΔ, τα δεδομένα αυτά θα μπορούσαν να αποτελέσουν αντικείμενο επεξεργασίας βάσει ενός από τους λόγους του άρθρου 6, υπό τον όρο ότι πληρούται μία από τις δύο εναλλακτικές πρόσθετες προϋποθέσεις:

(i) η επεξεργασία πρέπει να γίνεται υπό τον έλεγχο της δημόσιας αρχής, ή
(ii) Η επεξεργασία επιτρέπεται από το δίκαιο της ΕΕ / κράτους μέλους που προβλέπει κατάλληλες διασφαλίσεις για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων.

Υπάρχει αβεβαιότητα γύρω από τη διάταξη αυτή, διότι δεν είναι σαφές πώς ισχύουν οι δύο πρόσθετες απαιτήσεις που καθορίζονται σε αυτήν μαζί με το άρθρο 6. Η συντηρητική ερμηνεία είναι ότι οι ιδιωτικοί ή εμπορικοί φορείς δεν μπορούσαν να επεξεργαστούν τα δεδομένα αυτά, με άλλα λόγια «δεν υπάρχει περιθώριο στον κανονισμό για ιδιωτική ή εμπορική επεξεργασία αυτών των δεδομένων»[xi]. Η άλλη ερμηνεία είναι ότι τέτοιου είδους δεδομένα θα μπορούσαν να υποβληθούν σε επεξεργασία με όλους τους πιθανούς νομικούς λόγους υπό τον όρο ότι πληρούνται οι πρόσθετοι όροι (υπό τον έλεγχο της δημόσιας αρχής ή εάν επιτρέπονται βάσει του εφαρμοστέου δικαίου). Στο δόγμα αναφέρεται ότι η διάταξη αυτή θα οδηγήσει πιθανότατα σε συνεχιζόμενη εθνική απόκλιση[xii]. Αν και οι τοπικές αρχές θα λειτουργήσουν ως δημόσιες αρχές και θεωρητικά θα μπορούσαν να δικαιολογήσουν την πρώτη πρόσθετη απαίτηση για επεξεργασία (υπό τον έλεγχο της δημόσιας αρχής), θα ήταν σκόπιμο να εξεταστούν προσεκτικά οι τοπικοί κανονισμοί όταν τέτοιοι τύποι δεδομένων θα μπορούσαν να επεξεργαστούν (ιδίως στο πλαίσιο των δραστηριοτήτων στον τομέα του ανθρώπινου δυναμικού και της συλλογής ποινικών μητρώων, δεδομένου ότι οι αντίστοιχες πράξεις της Τοπικής Αρχής ενεργεί ως εργοδότης στο πλαίσιο αυτό παρά σαν κάτοχος δημόσιας εξουσίας και η δυνατότητα εφαρμογής της πρώτης πρόσθετης κατάστασης είναι αμφισβητήσιμη).

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

3. ΝΟΜΙΚΟΙ ΛΟΓΟΙ ΓΙΑ ΤΗΝ ΕΠΕΞΕΡΓΑΣΙΑ ΕΙΔΙΚΩΝ ΚΑΤΗΓΟΡΙΩΝ ΠΡΟΣΩΠΙΚΩΝ ΔΕΔΟΜΕΝΩΝ

Η γενική απαγόρευση επεξεργασίας ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα δεν ισχύει, υπό την προϋπόθεση ότι πληρείται μία από τις εναλλακτικές προϋποθέσεις που αναφέρονται κατωτέρω:

3.1. Ρητή συναίνεση

Οι απαιτήσεις που πρέπει να πληρούνται στο πλαίσιο του ΓΚΠΔ για να υπάρξει έγκυρη συναίνεση (ελεύθερη, συγκεκριμένη, εν επιγνώσει, ρητή) ισχύει σε κάθε περίπτωση για την επεξεργασία προσωπικών δεδομένων ειδικών κατηγοριών. Το στοιχείο «explicit» δεν ορίζεται στο ΓΚΠΔ. Η ομάδα εργασίας του άρθρου 29 (WP29) ανέφερε ότι απαιτείται ρητή συγκατάθεση σε καταστάσεις όπου εμφανίζεται σοβαρός κίνδυνος προστασίας δεδομένων και ότι είναι σκόπιμο υψηλό επίπεδο ατομικού ελέγχου των δεδομένων προσωπικού χαρακτήρα[xiii].

Ο όρος «ρητή» αναφέρεται στον τρόπο με τον οποίο εκφράζεται η συναίνεση από το υποκείμενο των δεδομένων - το υποκείμενο των δεδομένων πρέπει να δώσει ρητή δήλωση συγκατάθεσης [xiv]. Ένας από τους τρόπους να δοθεί συναίνεση είναι να επιβεβαιωθεί ρητά σε γραπτή δήλωση. Σε διαδικτυακό πλαίσιο, θα μπορούσαν να εφαρμοστούν διάφορες λύσεις συμπληρώνοντας μια ηλεκτρονική φόρμα, στέλνοντας ένα μήνυμα ηλεκτρονικού ταχυδρομείου, φορτώνοντας ένα σαρωμένο έγγραφο με την υπογραφή του υποκειμένου των δεδομένων ή χρησιμοποιώντας μια ηλεκτρονική υπογραφή. Οποιοδήποτε άλλο μέσο που θα επέτρεπε στον ελεγκτή για να αποδείξει το υψηλό όριο για τον τρόπο που πρέπει να δοθεί η συναίνεση θα ήταν σκόπιμο.

Δεδομένης της ανισορροπίας των εξουσιών μεταξύ των υποκειμένων των δεδομένων και των δημόσιων αρχών, δεν είναι ορθό οι τοπικές αρχές να βασίζονται κυρίως στη ρητή συναίνεση για την επεξεργασία ειδικών κατηγοριών προσωπικών δεδομένων (συμπεριλαμβανομένων και των σχέσεων με τους πολίτες και τους υπαλλήλους).

3.2. Υποχρεώσεις / ειδικά δικαιώματα στον τομέα της απασχόλησης, της κοινωνικής ασφάλισης και της νομοθεσίας κοινωνικής προστασίας

Αυτός ο όρος είναι ιδιαίτερα σημαντικός για τις Τοπικές Αρχές κατά τη διαχείριση της εσωτερικής επεξεργασίας Ανθρώπινου Δυναμικού. Η επεξεργασία ειδικών κατηγοριών προσωπικών δεδομένων μπορεί να είναι αναγκαία σε κάθε στάδιο της εργασιακής σχέσης - από την εμφάνισή της (διαδικασία πρόσληψης νέου προσωπικού), μέσω της εκτέλεσης, της τροποποίησής της και τελικά τον τερματισμό της.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

Παραδείγματα όπου μπορεί να είναι αναγκαία αυτή η επεξεργασία είναι τα εξής: η χορήγηση αναρρωτικών αδειών, αδειών μητρότητας, η μεταφορά ενός υπαλλήλου σε μια πιο κατάλληλη θέση λόγω θεμάτων υγείας κατόπιν αιτήματος των αρχών υγειονομικής περίθαλψης · τη συμμόρφωση με τους υποχρεωτικούς κανόνες που προβλέπουν ειδική προστασία για ορισμένες κατηγορίες εργαζομένων σε περίπτωση τερματισμού της εργασιακής σχέσης κλπ.

Οι γενικές απαιτήσεις που εισήχθησαν στον ΓΚΠΔ για τις εφαρμογές αυτού του λόγου είναι:

(i) Η επεξεργασία πρέπει να είναι απαραίτητη για την εκπλήρωση υποχρέωσης του υπεύθυνου επεξεργασίας δεδομένων ή ενός συγκεκριμένου δικαιώματος του υποκειμένου των δεδομένων

(ii) Αυτή η υποχρέωση / δικαίωμα θα μπορούσε να προβλεφθεί στο δίκαιο της ΕΕ/κράτους μέλους ή σε συλλογική (διαπραγματευτική) συμφωνία

(iii) Θα πρέπει να υπάρχουν οι κατάλληλες διασφαλίσεις για τα θεμελιώδη δικαιώματα και τα συμφέροντα του υποκειμένου των δεδομένων.

Προκειμένου να εφαρμοστεί αυτός ο νομικός λόγος, πρέπει να τηρείται η ειδική εθνική νομοθεσία του αντίστοιχου κράτους μέλους, όπου η Τοπική Αρχή λειτουργεί ως εργοδότης. Δεδομένου ότι ο νόμος περί απασχόλησης είναι ένας από τους τομείς στους οποίους ο ΓΚΠΔ εξουσιοδοτεί τα κράτη μέλη να υιοθετήσουν πρόσθετη νομοθεσία όσον αφορά την προστασία των προσωπικών δεδομένων (άρθρο 88), συνιστάται μια προσέγγιση σε τοπικό επίπεδο για τις Τοπικές Αρχές κατά την εφαρμογή αυτού του λόγου.

3.3. Ζωτικά συμφέροντα του υποκειμένου των δεδομένων ή άλλου φυσικού προσώπου

Παρόμοια με τον νομικό λόγο του άρθρου. 6, παράγραφος 1, στοιχείο «δ» του ΓΚΠΔ, τέτοιες καταστάσεις αναφέρονται σε συνθήκες ζωής ή θανάτου[xv]. Το ζωτικό συμφέρον μπορεί να είναι είτε το πρόσωπο στο οποίο αναφέρονται τα δεδομένα είτε άλλο πρόσωπο. Το διαφορετικό σε σχέση με το άρθρο 6 είναι ότι ο υπεύθυνος της επεξεργασίας φέρει το βάρος να αποδείξει την ύπαρξη πρόσθετης προϋπόθεσης, δηλαδή ότι «το πρόσωπο στο οποίο αναφέρονται τα δεδομένα είναι φυσικά ή νομικά ανίκανο να δώσει τη συγκατάθεσή του». Αυτή η διατύπωση συνεπάγεται ότι ο υπεύθυνος επεξεργασίας πρέπει να προσπαθήσει να λάβει πρώτα τη συγκατάθεση του υποκειμένου των δεδομένων.[xvi].

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

3.4. Επεξεργασία από μη κερδοσκοπικό σώμα με πολιτικό, φιλοσοφικό, θρησκευτικό ή συνδικαλιστικό σκοπό

Η δυνατότητα επεξεργασίας ευαίσθητων δεδομένων στο πλαίσιο αυτού του νομικού πλαισίου παρέχεται σε ορισμένους μη κερδοσκοπικούς οργανισμούς όπως πολιτικά κόμματα, ιδρύματα, εκκλησίες, άλλες μορφές φιλοσοφικών, θρησκευτικών ή συνδικαλιστικών οργανώσεων.

Οι οργανισμοί αυτοί θα μπορούσαν να επεξεργάζονται ευαίσθητα δεδομένα εάν

(i) τα δεδομένα αυτά αφορούν αποκλειστικά τα μέλη / πρώην μέλη του σώματος ή τα πρόσωπα που έχουν τακτική επαφή με αυτό
(ii) η επεξεργασία πραγματοποιείται στο πλαίσιο των νόμιμων δραστηριοτήτων τους
(iii) η επεξεργασία πραγματοποιείται σε σχέση με τους ειδικούς σκοπούς τους
(iv) υπάρχουν κατάλληλα μέτρα διασφάλισης για τα δικαιώματα του υποκειμένου των δεδομένων
(v) τα προσωπικά δεδομένα δεν αποκαλύπτονται εκτός αυτού του φορέα χωρίς τη συγκατάθεση των υποκειμένων των δεδομένων.

Άλλες ειδικές απαιτήσεις πρέπει να αναζητηθούν στο εθνικό δίκαιο[xvii].

Αυτός ο νομικός λόγος δεν θα είχε σχεδόν καμία πρακτική εφαρμογή για τις Τοπικές Αρχές κατά τη διάρκεια της δραστηριότητάς τους.

3.5. Τα δεδομένα δημοσιοποιούνται εμφανώς από το υποκείμενο των δεδομένων

Εάν τα δεδομένα προσωπικού χαρακτήρα αποκαλύπτονται εμφανώς στο ευρύ κοινό από το υποκείμενο των δεδομένων, τότε συμπεραίνεται ότι το υποκείμενο των δεδομένων έχει παραιτηθεί από την ειδική προστασία που παρέχεται σε τέτοιες πληροφορίες. Σε κάθε περίπτωση, η απόφαση αποκάλυψης τέτοιων πληροφοριών πρέπει να είναι αποτέλεσμα της ελεύθερης επιλογής του ατόμου[xviii]. Η αποκάλυψη αυτή μπορεί να λάβει διάφορες μορφές - δεδομένα από δημόσια διαθέσιμα μητρώα, ιστοσελίδες, λίστες, φόρουμ ή ακόμη και από ένα προφίλ σε ένα κοινωνικό δίκτυο που είναι προσβάσιμο χωρίς λογαριασμό χρήστη κ.λπ.[xix] Σε κάθε περίπτωση, το γεγονός ότι τα δεδομένα αυτά δημοσιοποιούνται προδήλως δεν απαλλάσσει τον υπεύθυνο επεξεργασίας από την υποχρέωση συμμόρφωσης με τις λοιπές απαιτήσεις του ΓΚΠΔ - π.χ. τήρηση των αρχών προστασίας δεδομένων, τήρηση της προστασίας της ιδιωτικής ζωής και προστασία της ιδιωτικής ζωής με σχεδιασμό, λήψη κατάλληλων μέτρων για την εγγύηση της ασφάλειας των δεδομένων κ.λπ.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

3.6. Ίδρυση, άσκηση ή υπεράσπιση νομικών αξιώσεων / δικαστηρίων που ενεργούν υπό την νομική τους ιδιότητα

Σε ορισμένες περιπτώσεις, η επεξεργασία ευαίσθητων δεδομένων μπορεί να είναι απαραίτητη για τον έλεγχο καθιέρωσης, άσκησης ή υπεράσπισης νομικών απαιτήσεων. Ο ελεγκτής φέρει το βάρος να αποδείξει ότι υπάρχει ανάγκη για τέτοια επεξεργασία, δηλαδή ότι υπάρχει στενή και ουσιαστική σύνδεση μεταξύ της επεξεργασίας και των σκοπών[xx]. Τέτοιες καταστάσεις μπορεί να περιλαμβάνουν π.χ. την άσκηση προσφυγής ενώπιον των διοικητικών δικαστηρίων για πράξεις που εκδίδονται από τις Τοπικές Αρχές όταν η επεξεργασία ευαίσθητων δεδομένων πραγματοποιήθηκε κατά την προηγούμενη διοικητική διαδικασία · εργασιακές διαφορές όπου τα δεδομένα υγείας των εργαζομένων που θα έπρεπε η Τοπική Αρχή να λάβει υπόψη ως εργοδότης κ.λπ.

Επιπλέον, η επεξεργασία στο πλαίσιο των νομικών δραστηριοτήτων δικαστηρίων θα μπορούσε επίσης να τεκμηριώνει την επεξεργασία τέτοιων κατηγοριών προσωπικών δεδομένων.

3.7. Ουσιώδες δημόσιο συμφέρον βάσει του δικαίου της ΕΕ ή των κρατών μελών

Η διάταξη αυτή του ΓΚΠΔ επιτρέπει στα κράτη μέλη να εισάγουν στην εθνική τους νομοθεσία συγκεκριμένη υπόθεση όπου θα μπορούσαν να επεξεργαστούν ευαίσθητα δεδομένα που να δικαιολογούν την επεξεργασία αυτή με σημαντικό δημόσιο συμφέρον.

Σε κάθε περίπτωση, για να ανταποκριθούν στις απαιτήσεις της GDPR, τα κράτη μέλη πρέπει να διασφαλίσουν ότι:

(i) η επεξεργασία πρέπει να είναι ανάλογη προς τον επιδιωκόμενο στόχο ·
(ii) τηρήθηκε η ουσία του δικαιώματος προστασίας δεδομένων ·
(iii) η εγκριθείσα νομοθεσία προβλέπει κατάλληλα και ειδικά μέτρα για τη διασφάλιση των θεμελιωδών δικαιωμάτων και των συμφερόντων του υποκειμένου των δεδομένων.

Παραμένει να δούμε πώς θα χρησιμοποιηθεί αυτή η ευκαιρία στο μέλλον. Μια ανάλυση κατά περίπτωση του αντίστοιχου τοπικού νόμου είναι ενδεδειγμένη για τις Τοπικές Αρχές προκειμένου να διαπιστωθεί αν μπορούν να στηριχθούν σε αυτό το έδαφος.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

3.8. Προληπτική ή επαγγελματική ιατρική, εκτίμηση της εργασιακής ικανότητας του εργαζομένου, ιατρική διάγνωση, παροχή υγειονομικής ή κοινωνικής φροντίδας ή θεραπείας

Η απαγόρευση επεξεργασίας ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα δεν ισχύει για σκοπούς ιατρικής / κοινωνικής φροντίδας[xxi]. Η επεξεργασία αυτή μπορεί να πραγματοποιηθεί σε διάφορους τομείς όπως η επαγγελματική ιατρική, η ιατρική διάγνωση ή η παροχή υπηρεσιών στον τομέα της κοινωνικής ή ιατρικής περίθαλψης. Η επεξεργασία αυτή μπορεί να γίνει είτε βάσει του δικαίου της ΕΕ / κράτους μέλους είτε βάσει σύμβασης με τον επαγγελματία υγείας[xxii]. Επιπλέον, το άρθρο. 9, παρ. 3 του GDPR επιτρέπει την επεξεργασία ευαίσθητων δεδομένων από πρόσωπο που δεσμεύεται από το επαγγελματικό απόρρητο.

Αυτός ο νομικός λόγος ισχύει για τους γιατρούς, τους νοσηλευτές και άλλα πρόσωπα που εμπλέκονται στην παροχή υπηρεσιών υγειονομικής περίθαλψης[xxiii].

Από πρακτική άποψη, η διάταξη αυτή θα επιτρέψει στις τοπικές αρχές με την ιδιότητά τους ως εργοδότες να εξασφαλίζουν υπηρεσίες επαγγελματικής ιατρικής ως μέρος της μεγαλύτερης υποχρέωσης να εξασφαλίσουν καλές συνθήκες εργασίας για την υγεία και την ασφάλεια.

3.9. Το δημόσιο συμφέρον στον τομέα της δημόσιας υγείας

Σύμφωνα με την αιτιολογική σκέψη 54 του ΓΚΠΔ, η «δημόσια υγεία» πρέπει να ερμηνεύεται σύμφωνα με τον ορισμό του κανονισμού (ΕΚ) αριθ. 1338/2008, δηλαδή όλα τα στοιχεία που αφορούν την υγεία, την κατάσταση της υγείας, συμπεριλαμβανομένης της νοσηρότητας και της αναπηρίας, την υγειονομική κατάσταση, τις ανάγκες υγειονομικής περίθαλψης, τους πόρους που διατίθενται για την υγειονομική περίθαλψη, την παροχή και την καθολική πρόσβαση στην υγειονομική περίθαλψη, καθώς και τις δαπάνες και τη χρηματοδότηση της υγειονομικής περίθαλψης, καθώς και τα αίτια θνησιμότητας.

Λόγοι που θα μπορούσαν να δικαιολογήσουν την εφαρμογή αυτού του νομικού πλαισίου θα μπορούσαν να είναι η προστασία από σοβαρές διασυνοριακές απειλές κατά της υγείας ή η διασφάλιση υψηλού επιπέδου ποιότητας και ασφάλειας της υγειονομικής περίθαλψης, των ιατρικών προϊόντων ή των ιατροτεχνολογικών προϊόντων[xxiv].

Η επεξεργασία δεδομένων υγείας για λόγους δημοσίου συμφέροντος δεν θα πρέπει να έχει ως αποτέλεσμα την επεξεργασία δεδομένων προσωπικού χαρακτήρα για άλλους σκοπούς από τρίτους, όπως εργοδότες ή ασφαλιστικές και τραπεζικές εταιρείες.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

3.10. Επεξεργασία για αρχειοθετικούς σκοπούς γενικού συμφέροντος, επιστημονικούς ή ιστορικούς σκοπούς ή στατιστικούς σκοπούς

Η επεξεργασία για τους σκοπούς αυτούς θα πρέπει να βασίζεται στο δίκαιο των κρατών μελών / της ΕΕ. Ο ΓΚΠΔ απαιτεί οι νομοθετικές διατάξεις που επιτρέπουν αυτή την επεξεργασία να είναι: αναλογικές προς τον επιδιωκόμενο στόχο, να σέβονται την ουσία του δικαιώματος προστασίας των δεδομένων και να προβλέπουν κατάλληλα και ειδικά μέτρα για τη διασφάλιση των θεμελιωδών δικαιωμάτων και των συμφερόντων του υποκειμένου των δεδομένων. Οι διασφαλίσεις που εισάγονται πρέπει να αντιστοιχούν στον ευαίσθητο χαρακτήρα των σχετικών δεδομένων προσωπικού χαρακτήρα[xxv].

3.11. Περαιτέρω προϋποθέσεις στο δίκαιο των κρατών μελών

Το άρθρο 9 παράγραφος 4 του ΓΚΠΔ εξουσιοδοτεί τα κράτη μέλη να θεσπίσουν περαιτέρω όρους ή περιορισμούς για την επεξεργασία ορισμένων ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα, συγκεκριμένα: γενετικά δεδομένα, βιομετρικά δεδομένα ή δεδομένα σχετικά με την υγεία. Συνεπώς, η τοπική νομοθεσία που εφαρμόζεται στις Τοπικές Αρχές θα πρέπει να παρακολουθείται στο μέλλον.

4. ΣΥΜΠΕΡΑΣΜΑ ΚΑΙ ΠΡΑΚΤΙΚΕΣ ΣΥΜΒΟΥΛΕΣ

Οι Τοπικές Αρχές πρέπει να γνωρίζουν ότι ορισμένες κατηγορίες δεδομένων προσωπικού χαρακτήρα χρήζουν ιδιαίτερης προστασίας, διότι συνδέονται εγγενώς με τις πιο οικείες ιδιωτικές σφαίρες ή / και ενέχουν τον κίνδυνο διακρίσεων. Κατά γενικό κανόνα, η επεξεργασία τέτοιων δεδομένων απαγορεύεται, εκτός εάν υπάρχουν πρόσθετοι όροι (εξαιρέσεις από αυτόν τον κανόνα).

Οι πιο πρακτικές πτυχές που ενδέχεται να επηρεάσουν τις δραστηριότητες των Τοπικών Αρχών είναι οι δραστηριότητες επεξεργασίας δεδομένων υγείας των εργαζομένων. Ο ΓΚΠΔ επιτρέπει την επεξεργασία αυτή, αλλά μόνο εάν είναι απαραίτητο για την υποχρέωση του ελεγκτή (ή το δικαίωμα του υποκειμένου δεδομένων) σύμφωνα με το εργατικό δίκαιο.

Τα στοιχεία σχετικά με τις ποινικές καταδίκες και τα αδικήματα δεν είναι ειδική κατηγορία, αλλά υπάγονται επίσης σε ειδικό καθεστώς βάσει του ΓΚΠΔ. Οι πρακτικές του Ανθρώπινου Δυναμικού για τη συλλογή ποινικών μητρώων ή την διεξαγωγή εκτεταμένων ελέγχων ιστορικού των μελλοντικών υπαλλήλων θα πρέπει να αναθεωρηθεί υπό το πρίσμα του ΓΚΠΔ.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

5. ΕΞΩΤΕΡΙΚΕΣ ΠΗΓΕΣ & ΔΙΑΔΙΚΤΥΑΚΟΙ ΣΥΝΔΕΣΜΟΙ

Βιβλία

- **Boardman, R., Mullock, J., Mole, A.** Bird & Bird Guide to General Data Protection Regulation (2016);
- **Ehmann, E., Helfrich, M.** EG Datenschutzrichtlinie: Kurzkommentar, Verlag Dr. Otto Schmidt, Koln, (1999)
- **Voigt, P., von dem Bussche, A.**, The EU General Data Protection Regulation (GDPR) – A Practical Guide, Springer International Publishing (2017);
- **EU** General Data Protection Regulation (GDPR). An Implementation and Compliance Guide, IT Governance Publishing, Cambridgeshire (2016);
- **European** Data Protection. Law and Practice, Executive Editor: Edurado Ustaran, CIPP/E, Partner, Hogan Lovells, IAPP (2018);

Έγγραφα της ομάδας εργασίας του άρθρου 29

- WP29, Guidelines on Consent under Regulation 2016/679, WP 259;
- WP29, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, WP 217;

Διαδικτυακοί Σύνδεσμοι

- http://europa.eu/rapid/press-release_IP-18-386_en.htm
- https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en
- https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/sensitive-data/what-personal-data-considered-sensitive_en
- https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/sensitive-data/under-what-conditions-can-my-company-organisation-process-sensitive-data_en

6. ΠΑΡΑΠΟΜΠΕΣ

[i] Ehmann, E., Helfrich, M. EG Datenschutzrichtlinie: Kurzkommentar, Verlag Dr. Otto Schmidt, Koln, (1999), p. 130-131.
[ii] GDPR explicitly recognizes the term 'sensitive data' – see e.g. Recital 10.
[iii] European Data Protection. Law and Practice, Executive Editor: Edurado Ustaran, CIPP/E, Partner, Hogan Lovells, IAPP (2018), p. 123.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

[iv] Voigt, P., von dem Bussche, A., The EU General Data Protection Regulation (GDPR) – A Practical Guide, Springer International Publishing (2017), p. 111.
[v] Ibid, p. 111.
[vi] Ibid, p. 111.
[vii] In Bulgaria such data are sensitive since 2005.
[viii] Boardman, R., Mullock, J., Mole, A. Bird & Bird Guide to General Data Protection Regulation (2016), p. 18.
[ix] Voigt, P., von dem Bussche, A., The EU General Data Protection Regulation (GDPR) – A Practical Guide, Springer International Publishing (2017), p. 111.
[x] Boardman, R., Mullock, J., Mole, A. Bird & Bird Guide to General Data Protection Regulation (2016), p. 19.
[xi] EU General Data Protection Regulation (GDPR). An Implementation and Compliance Guide, IT Governance Publishing, Cambridgeshire (2016), p. 196.
[xii] Boardman, R., Mullock, J., Mole, A. Bird & Bird Guide to General Data Protection Regulation (2016), p. 19.
[xiii] WP29, Guidelines on Consent under Regulation 2016/679, WP 259, p. 18.
[xiv] Ibid, p. 18.
[xv] European Data Protection. Law and Practice, Executive Editor: Edurado Ustaran, CIPP/E, Partner, Hogan Lovells, IAPP (2018), p. 126.
[xvi] Ibid, p. 126.
[xvii] Ibid, p. 126-127.
[xviii] Voigt, P., von dem Bussche, A., The EU General Data Protection Regulation (GDPR) – A Practical Guide, Springer International Publishing (2017), p. 113.
[xix] Ibid, p. 113.
[xx] European Data Protection. Law and Practice, Executive Editor: Edurado Ustaran, CIPP/E, Partner, Hogan Lovells, IAPP (2018), p. 127.
[xxi] Ibid, p. 128.
[xxii] Ibid, p. 129.
[xxiii] Ibid, p. 129.
[xxiv] Voigt, P., von dem Bussche, A., The EU General Data Protection Regulation (GDPR) – A Practical Guide, Springer International Publishing (2017), p. 114.
[xxv] Ibid, p. 115.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

ProLegis

Διορισμός, θέση και καθήκοντα των Υπεύθυνων Προστασίας Δεδομένων (ΥΠΔ)

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

ProLegis

Contents

1. ΝΟΜΙΚΟ ΠΛΑΙΣΙΟ 4

Γενικός Κανονισμός Προστασίας Δεδομένων (ΓΚΠΔ) 4

2. ΔΙΟΡΙΣΜΟΣ ΤΟΥ ΥΠΕΥΘΥΝΟΥ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ (ΥΠΔ) 8

2.1. Υποχρεωτικός διορισμός σύμφωνα με το ΓΚΠΔ 8

2.1.1. Δημόσια αρχή ή οργανισμός 8

2.1.2. Οι βασικές δραστηριότητες του ελεγκτή / επεξεργαστή [...] απαιτούν τακτική και συστηματική παρακολούθηση των υποκειμένων των δεδομένων σε μεγάλη κλίμακα 9

2.1.3. Οι κύριες δραστηριότητες του ελεγκτή / επεξεργαστή συνίστανται στην ευρείας κλίμακας ειδικών κατηγοριών δεδομένων [...] και σε δεδομένα προσωπικού χαρακτήρα που αφορούν ποινικές καταδίκες και αξιόποινες πράξεις 10

2.2. Άλλες καταστάσεις για τον ορισμό του DPO 11

2.2.1. Υποχρεωτικός διορισμός βάσει της νομοθεσίας της ΕΕ / των κρατών μελών 11

2.2.2. Εθελούσιος διορισμός 11

2.3. Συμβατικές σχέσεις με τον ΥΠΔ 12

2.3.1. Σύμβαση εργασίας 12

2.3.2. Σύμβαση παροχής υπηρεσιών 12

3. ΘΕΣΗ ΤΟΥ ΥΠΔ 13

3.1. Συμμετοχή σε όλα τα θέματα που σχετίζονται με την προστασία των προσωπικών δεδομένων 13

3.2. Διασφάλιση αναγκαίων πόρων και ανεξαρτησία 13

3.3. Σύγκρουση συμφερόντων 15

4. ΚΑΘΗΚΟΝΤΑ ΤΟΥ ΥΠΔ 16

4.1. Παρακολούθηση 16

4.2. Αξιολόγηση των Επιπτώσεων της Προστασίας Δεδομένων (ΑΕΠΔ) 16

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

4.3. Σημείο επαφής 16
4.4. Τήρηση αρχείων 17
5. ΣΥΜΠΕΡΑΣΜΑ ΚΑΙ ΠΡΑΚΤΙΚΕΣ ΣΥΜΒΟΥΛΕΣ 17
6. ΕΞΩΤΕΡΙΚΕΣ ΠΗΓΕΣ & ΔΙΑΔΙΚΤΥΑΚΟΙ ΣΥΝΔΕΣΜΟΙ 19
Βιβλία 19
Έγγραφα της ομάδας εργασίας του άρθρου 29 19
Διαδικτυακοί Σύνδεσμοι 19
7. ΠΑΡΑΠΟΜΠΕΣ 19

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

1. ΝΟΜΙΚΟ ΠΛΑΙΣΙΟ

Γενικός Κανονισμός Προστασίας Δεδομένων (ΓΚΠΔ)

Αιτιολογική Σκέψη (97)

Εάν η επεξεργασία διενεργείται από δημόσια αρχή, εξαιρουμένων των δικαστηρίων ή των ανεξάρτητων δικαστικών αρχών όταν ενεργούν υπό τη δικαιοδοτική τους αρμοδιότητα, εφόσον, στον ιδιωτικό τομέα, η επεξεργασία διενεργείται από υπεύθυνο επεξεργασίας του οποίου οι βασικές δραστηριότητες περιλαμβάνουν πράξεις επεξεργασίας οι οποίες απαιτούν τακτική και συστηματική παρακολούθηση των υποκειμένων των δεδομένων σε μεγάλη κλίμακα, ή εάν οι βασικές δραστη ριότητες του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία συνιστούν μεγάλης κλίμακας επεξεργασία ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα και δεδομένων που αφορούν ποινικές καταδίκες και αδικήματα, L 119/18 EL Επίσημη Εφημερίδα της Ευρωπαϊκής Ένωσης 4.5.2016 ένα πρόσωπο με ειδικές γνώσεις στο δίκαιο και στις πρακτικές προστασίας των δεδομένων θα πρέπει να παρέχει συνδρομή στον υπεύθυνο επεξεργασίας ή τον εκτελούντα την επεξεργασία κατά την παρακολούθηση της εσωτερικής συμμόρφωσης προς τον παρόντα κανονισμό. Στον ιδιωτικό τομέα, οι βασικές δραστηριότητες ενός υπευθύνου επεξεργασίας αφορούν τις κύριες δραστηριότητές του και όχι την επεξεργασία δεδομένων προσωπικού χαρακτήρα ως παρεπόμενη δραστηριότητα. Το αναγκαίο επίπεδο εμπειρίας θα πρέπει να καθορίζεται ειδικότερα ανάλογα με τις πράξεις επεξεργασίας δεδομένων που διενεργούνται και από την προστασία την οποία απαιτούν τα δεδομένα προσωπικού χαρακτήρα που επεξεργάζονται ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία. Οι εν λόγω υπεύθυνοι προστασίας δεδομένων, ανεξάρτητα από το κατά πόσον είναι υπάλληλοι του υπευθύνου επεξεργασίας, θα πρέπει να είναι σε θέση να εκτελούν τις υποχρεώσεις και τα καθήκοντά τους με ανεξάρτητο τρόπο.

Άρθρο 37

Ορισμός του υπευθύνου προστασίας δεδομένων

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

1. Ο υπεύθυνος επεξεργασίας και ο εκτελών την επεξεργασία ορίζουν υπεύθυνο προστασίας δεδομένων σε κάθε περίπτωση στην οποία:

(a) η επεξεργασία διενεργείται από δημόσια αρχή ή φορέα, εκτός από δικαστήρια που ενεργούν στο πλαίσιο της δικαιοδοτικής τους αρμοδιότητας;

(b) οι βασικές δραστηριότητες του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία συνιστούν πράξεις επεξεργασίας οι οποίες, λόγω της φύσης, του πεδίου εφαρμογής και/ή των σκοπών τους, απαιτούν τακτική και συστηματική παρακολούθηση των υποκειμένων των δεδομένων σε μεγάλη κλίμακα, ή

(c) οι βασικές δραστηριότητες του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία συνιστούν μεγάλης κλίμακας επεξεργασία ειδικών κατηγοριών δεδομένων προσωπικού χαρακτήρα κατά το άρθρο 9 και δεδομένων που αφορούν ποινικές καταδίκες και αδικήματα που αναφέρονται στο άρθρο 10.

2. Όμιλος επιχειρήσεων μπορεί να διορίσει ένα μόνο υπεύθυνο προστασίας δεδομένων, υπό την προϋπόθεση ότι κάθε εγκατάσταση έχει εύκολη πρόσβαση στον υπεύθυνο προστασίας δεδομένων.

3. Εάν ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία είναι δημόσια αρχή ή δημόσιος φορέας, ένας μόνο υπεύθυνος προστασίας δεδομένων μπορεί να ορίζεται για πολλές τέτοιες αρχές ή πολλούς τέτοιους φορείς, λαμβάνοντας υπόψη την οργανωτική τους δομή και το μέγεθός τους.

4. Σε περιπτώσεις πλην των αναφερόμενων στην παράγραφο 1, ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία ή ενώσεις και άλλοι φορείς που εκπροσωπούν κατηγορίες υπευθύνων επεξεργασίας ή εκτελούντων την επεξεργασία μπορούν να ορίζουν υπεύθυνο προστασίας δεδομένων ή, όπου απαιτείται από το δίκαιο της Ένωσης ή του κράτους μέλους, ορίζουν υπεύθυνο προστασίας δεδομένων. Ο υπεύθυνος προστασίας δεδομένων μπορεί να ενεργεί για τις εν λόγω ενώσεις και τους άλλους φορείς που εκπροσωπούν υπευθύνους επεξεργασίας ή εκτελούντες την επεξεργασία .

5. Ο υπεύθυνος προστασίας δεδομένων διορίζεται βάσει επαγγελματικών προσόντων και ιδίως βάσει της εμπειρογνωσίας που διαθέτει στον τομέα του δικαίου και των πρακτικών περί προστασίας δεδομένων, καθώς και βάσει της ικανότητας εκπλήρωσης των καθηκόντων που αναφέρονται στο άρθρο 39.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

6. Ο υπεύθυνος προστασίας δεδομένων μπορεί να είναι μέλος του προσωπικού του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία ή να ασκεί τα καθήκοντά του βάσει σύμβασης παροχής υπηρεσιών.

7. Ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία δημοσιεύουν τα στοιχεία επικοινωνίας του υπευθύνου προστασίας δεδομένων και τα ανακοινώνουν στην εποπτική αρχή.

Άρθρο 38

Θέση του υπευθύνου προστασίας δεδομένων

1. Ο υπεύθυνος επεξεργασίας και ο εκτελών την επεξεργασία διασφαλίζουν ότι ο υπεύθυνος προστασίας δεδομένων συμμετέχει, δεόντως και εγκαίρως, σε όλα τα ζητήματα τα οποία σχετίζονται με την προστασία δεδομένων προσωπικού χαρακτήρα.

2. Ο υπεύθυνος επεξεργασίας και ο εκτελών την επεξεργασία στηρίζουν τον υπεύθυνο προστασίας δεδομένων στην άσκηση των καθηκόντων που αναφέρονται στο άρθρο 39 παρέχοντας απαραίτητους πόρους για την άσκηση των εν λόγω καθηκόντων και πρόσβαση σε δεδομένα προσωπικού χαρακτήρα και σε πράξεις επεξεργασίας, καθώς και πόρους απαραίτητους για τη διατήρηση της εμπειρογνωσίας του.

3. Ο υπεύθυνος επεξεργασίας και ο εκτελών την επεξεργασία διασφαλίζει ότι ο υπεύθυνος προστασίας δεδομένων δεν λαμβάνει εντολές για την άσκηση των εν λόγω καθηκόντων. Δεν απολύεται ούτε υφίσταται κυρώσεις από τον υπεύθυνο επεξεργασίας ή τον εκτελούντα την επεξεργασία επειδή επιτέλεσε τα καθήκοντά του. Ο υπεύθυνος προστασίας δεδομένων λογοδοτεί απευθείας στο ανώτατο διοικητικό επίπεδο του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία.

4. Τα υποκείμενα των δεδομένων μπορούν να επικοινωνούν με τον υπεύθυνο προστασίας δεδομένων για κάθε ζήτημα σχετικό με την επεξεργασία των δεδομένων τους προσωπικού χαρακτήρα και με την άσκηση των δικαιωμάτων τους δυνάμει του παρόντος κανονισμού.

5. Ο υπεύθυνος προστασίας δεδομένων δεσμεύεται από την τήρηση του απορρήτου ή της εμπιστευτικότητας σχετικά με την εκτέλεση των καθηκόντων του, σύμφωνα με το δίκαιο της Ένωσης ή του κράτους μέλους.

6. Ο υπεύθυνος προστασίας δεδομένων μπορεί να επιτελεί και άλλα καθήκοντα και υποχρεώσεις. Ο υπεύθυνος επεξεργασίας ή ο εκτελών την επεξεργασία διασφαλίζουν

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

ότι τα εν λόγω καθήκοντα και υποχρεώσεις δεν συνεπάγονται σύγκρουση συμφερόντων.

Άρθρο 39

Καθήκοντα του υπευθύνου προστασίας δεδομένων

1. Ο υπεύθυνος προστασίας δεδομένων έχει τουλάχιστον τα ακόλουθα καθήκοντα:

(a) ενημερώνει και συμβουλεύει τον υπεύθυνο επεξεργασίας ή τον εκτελούντα την επεξεργασία και τους υπαλλήλους που επεξεργάζονται τις υποχρεώσεις τους που απορρέουν από τον παρόντα κανονισμό και από άλλες διατάξεις της Ένωσης ή του κράτους μέλους σχετικά με την προστασία δεδομένων,

(b) παρακολουθεί τη συμμόρφωση με τον παρόντα κανονισμό, με άλλες διατάξεις της Ένωσης ή του κράτους μέλους σχετικά με την προστασία δεδομένων και με τις πολιτικές του υπευθύνου επεξεργασίας ή του εκτελούντος την επεξεργασία σε σχέση με την προστασία των δεδομένων προσωπικού χαρακτήρα, συμπεριλαμβανομένων της ανάθεσης αρμοδιοτήτων, της ευαισθητο¬ ποίησης και της κατάρτισης των υπαλλήλων που συμμετέχουν στις πράξεις επεξεργασίας, και των σχετικών ελέγχων,

(c) παρέχει συμβουλές, όταν ζητείται, όσον αφορά την εκτίμηση αντικτύπου σχετικά με την προστασία των δεδομένων και παρακολουθεί την υλοποίησή της σύμφωνα με το άρθρο 35,

(d) συνεργάζεται με την εποπτική αρχή,

(e) ενεργεί ως σημείο επικοινωνίας για την εποπτική αρχή για ζητήματα που σχετίζονται με την επεξεργασία, περιλαμβανομένης της προηγούμενης διαβούλευσης που αναφέρεται στο άρθρο 36, και πραγματοποιεί διαβουλεύσεις, ανάλογα με την περίπτωση, για οποιοδήποτε άλλο θέμα.

2. Κατά την εκτέλεση των καθηκόντων του, ο υπεύθυνος προστασίας δεδομένων λαμβάνει δεόντως υπόψη τον κίνδυνο που συνδέεται με τις πράξεις επεξεργασίας, συνεκτιμώντας τη φύση, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς της επεξεργασίας.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

2. ΔΙΟΡΙΣΜΟΣ ΤΟΥ ΥΠΕΥΘΥΝΟΥ ΠΡΟΣΤΑΣΙΑΣ ΔΕΔΟΜΕΝΩΝ (ΥΠΔ)

2.1. Υποχρεωτικός διορισμός σύμφωνα με το ΓΚΠΔ

2.1.1. Δημόσια αρχή ή οργανισμός

Ο ΓΚΠΔ δεν περιέχει νομικό ορισμό που νοείται ως "δημόσια αρχή ή οργανισμός". Το κατά πόσον ένα φυσικό ή νομικό πρόσωπο αποτελεί δημόσια αρχή/οργανισμό πρέπει να ορίζεται σύμφωνα με την εθνική νομοθεσία κάθε κράτους μέλους. Η έννοια αυτή πρέπει να ερμηνεύεται **ευρέως** και, σε κάθε περίπτωση, περιλαμβάνει εθνικές, περιφερειακές και **τοπικές αρχές**. Ωστόσο, σύμφωνα με το WP29, ενδέχεται να περιλαμβάνονται και ορισμένα φυσικά/νομικά πρόσωπα των οποίων οι δραστηριότητες διέπονται από το δημόσιο/ιδιωτικό δίκαιο (π.χ. υπηρεσίες δημόσιων μεταφορών, ύδρευση και ενέργεια, οδικές υποδομές, δημόσιες ραδιοτηλεοπτικές υπηρεσίες, δημόσιες κατοικίες ή πειθαρχικά όργανα για το νομοθετικά κατοχυρωμένο επάγγελμα).[1] Η λογική πίσω από μια τέτοια ερμηνεία είναι ότι οι πολίτες (υποκείμενα των δεδομένων) έχουν περιορισμένη επιλογή για το εάν και πώς αυτοί οι φορείς θα επεξεργάζονται τα προσωπικά τους δεδομένα. Αν και η ερμηνεία αυτή δεν είναι υποχρεωτική και δεσμευτική, εντός αυτών των οργανώσεων σε περίπτωση που οριστεί ένας ΥΠΔ, απαιτείται προσεκτική εξέταση και ανάλυση.

Πρέπει να σημειωθεί ότι το WP29 συνιστά ως ορθή πρακτική τον ορισμό ενός ΥΠΔ του οποίου οι αρμοδιότητες πρέπει επίσης να καλύπτουν όλες τις εργασίες επεξεργασίας, συμπεριλαμβανομένων εκείνων που δεν σχετίζονται με την εκτέλεση δημόσιας αποστολής ή άσκησης υπηρεσιακού καθήκοντος (π.χ. υπαλλήλους)[i]. Ωστόσο, καμία από τις διατάξεις του ΓΚΠΔ δεν απαιτεί τον ορισμό του ΥΠΔ μόνο για τις δραστηριότητες επεξεργασίας που σχετίζονται με δημόσιες λειτουργίες. Έτσι, η λογικότερη και ασφαλέστερη ερμηνεία είναι ότι η Τοπική Αρχή διορίζει τον υπεύθυνο προστασίας δεδομένων **ο οποίος είναι υπεύθυνος για όλες τις δραστηριότητες επεξεργασίας δεδομένων** εντός του οργανισμού (σχέσεις με τους πολίτες, τους εργαζόμενους, τους υποψήφιους για εργασία, πρώην υπαλλήλους, άλλες δημόσιες αρχές κ.λπ.).

[1] WP29, Guidelines on Data Protection Officers ('DPOs'), WP 243 rev.01, p. 6.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

2.1.2. Οι βασικές δραστηριότητες του ελεγκτή / επεξεργαστή [...] απαιτούν τακτική και συστηματική παρακολούθηση των υποκειμένων των δεδομένων σε μεγάλη κλίμακα

Οι δραστηριότητες επεξεργασίας δεδομένων των Τοπικών Αρχών θα εμπίπτουν γενικά στο πεδίο εφαρμογής του σημείου 2.1.1. ανωτέρω, δηλαδή οι Τοπικές Αρχές θα πρέπει να ορίσουν υπεύθυνο προστασίας δεδομένων βάσει της ιδιότητάς τους ως δημόσιας αρχής/φορέα. Για λόγους σαφήνειας, παρακάτω θα γίνει μια σύντομη ανάλυση των δύο άλλων υποθέσεων στο πλαίσιο του ΓΚΠΔ όταν ο διορισμός του ΥΠΔ είναι υποχρεωτικός. Αυτές οι πληροφορίες μπορεί να είναι χρήσιμες για ιδιωτικές οντότητες των οποίων το κεφάλαιο ανήκει εν μέρει ή εξ ολοκλήρου στο Δήμο ή σε άλλους φορείς Τοπικών Αρχών / κράτους και οι οποίοι δεν εμπίπτουν στο πεδίο εφαρμογής της "δημόσιας αρχής / οργανισμού".

Κάτω από τον όρο "**βασικές δραστηριότητες**" πρέπει να κατανοήσουμε τις βασικές λειτουργίες που είναι απαραίτητες για την επίτευξη των στόχων του ελεγκτή ή του επεξεργαστή. [2]Παραδείγματα που παρασχέθηκαν από το WP29 περιλαμβάνουν την επεξεργασία των ιατρικών φακέλων στα νοσοκομεία ή της παρακολούθησης που διενεργείται από ιδιωτική εταιρεία ασφαλείας. Ταυτόχρονα, οι τυποποιημένες δραστηριότητες πληροφόρησης στον τομέα της πληροφορικής των εργαζομένων, αποκλείονται από τις "βασικές δραστηριότητες" του οργανισμού[ii].

Η έννοια "**ευρεία κλίμακα**" δεν ορίζεται ρητά στον ΓΚΠΔ. Αναφέρεται ρητά ότι η επεξεργασία σε περιφερειακό, εθνικό ή υπερεθνικό επίπεδο, η οποία περιλαμβάνει σημαντικό όγκο δεδομένων που θα μπορούσαν να επηρεάσουν μεγάλο αριθμό υποκειμένων των δεδομένων και οι οποίες είναι πιθανό να οδηγήσουν σε υψηλό κίνδυνο, θα μπορούσαν να θεωρηθούν ως επεξεργασία "ευρείας κλίμακας". Αντίθετα, οι ανεξάρτητοι επαγγελματίες όπως οι ειδικοί σε θέματα υγειονομικής περίθαλψης ή δικηγόροι δεν επεξεργάζονται δεδομένα προσωπικού χαρακτήρα σε "μεγάλη κλίμακα".

Σύμφωνα με το WP29, μια περιληπτική λίστα δραστηριοτήτων που μπορεί να θεωρηθεί ευρείας κλίμακας επεξεργασία περιλαμβάνει:

- επεξεργασία δεδομένων ασθενών από νοσοκομείο;
- επεξεργασία δεδομένων μετκίνησης ατόμων που χρησιμοποιούν δημόσιο σύστημα δημόσιας συγκοινωνίας (π.χ. παρακολούθηση μέσω ταξιδιωτικών καρτών);

[2] Ibid.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

- επεξεργασία δεδομένων γεωγραφικής θέσης σε πραγματικό χρόνο των πελατών μιας διεθνούς αλυσίδας fast food;
- για στατιστικούς σκοπούς από έναν Επεξεργαστή ειδικευμένο στην παροχή αυτών των υπηρεσιών;
- επεξεργασία δεδομένων πελατών από ασφαλιστική εταιρεία / τράπεζα;
- επεξεργασία προσωπικών δεδομένων για συμπεριφορική διαφήμιση μέσω μιας μηχανής αναζήτησης
- επεξεργασία δεδομένων (περιεχόμενο, κίνηση, τοποθεσία) από τηλεφωνικούς παρόχους υπηρεσιών ή αντίστοιχων παρόχων Διαδικτύου[iii].

Η έννοια "**τακτική**" είναι εγγενώς συνδεδεμένη με την επεξεργασία που γίνεται είτε μόνιμα (συνεχώς) είτε περιοδικά. Η έννοια "**συστηματική παρακολούθηση**" απαιτεί η επεξεργασία να πραγματοποιείται με ένα συγκεκριμένο σχέδιο, στρατηγική ή παρόμοια προκαθορισμένη μεθοδολογία, με οργανωμένο τρόπο μέσα σε ένα σύστημα.[3] Παραδείγματα περιλαμβάνουν, μεταξύ άλλων, φορείς εκμετάλλευσης δικτύων τηλεπικοινωνιών, σκιαγράφησης προφίλ, συμπεριφορική διαφήμιση, έξυπνες συσκευές κ.λπ.

2.1.3. Οι κύριες δραστηριότητες του ελεγκτή / επεξεργαστή συνίστανται στην ευρείας κλίμακας ειδικών κατηγοριών δεδομένων [...] και σε δεδομένα προσωπικού χαρακτήρα που αφορούν ποινικές καταδίκες και αξιόποινες πράξεις

Για τους όρους "βασικές δραστηριότητες" και "μεγάλης κλίμακας" βλέπε το σημείο 2.1.2. παραπάνω.

Ο όρος και θα πρέπει να ερμηνεύεται διορθωτικά ως "ή". Με άλλα λόγια, κάθε επεξεργασία που περιλαμβάνει είτε την επεξεργασία ειδικών κατηγοριών δεδομένων ή προσωπικών δεδομένων που αφορούν ποινικές καταδίκες και αδικήματα ευρείας κλίμακας και αποτελούν μέρος της βασικής δραστηριότητας της οργάνωσης, θα πρέπει να απαιτούν τον διορισμό του ΥΠΔ.

Ειδικές κατηγορίες δεδομένων είναι:

- τα δεδομένα προσωπικού χαρακτήρα που αποκαλύπτουν τη φυλετική ή εθνοτική καταγωγή;
- πολιτικές απόψεις;
- Θρησκευτικές ή φιλοσοφικές πεποιθήσεις;
- συμμετοχή σε συνδικαλιστικές οργανώσεις;

[3] See the exact interpretation made by WP29 in WP29, Guidelines on Data Protection Officers ('DPOs'), WP 243 rev.01, p. 8.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

- γενετικά δεδομένα;
- βιομετρικά δεδομένα για τον μοναδικό προσδιορισμό ενός φυσικού προσώπου:
- δεδομένα σχετικά με την υγεία ή τα δεδομένα σχετικά με τη σεξουαλική ζωή ή τον σεξουαλικό προσανατολισμό ενός φυσικού προσώπου.

Τα δεδομένα προσωπικού χαρακτήρα σχετικά με ποινικές καταδίκες και αξιόποινες πράξεις μπορούν να περιλαμβάνουν πληροφορίες που περιέχουν δικαστικές αποφάσεις, ποινικό μητρώο, πράξεις ελεγκτικών οργάνων.

2.2. Άλλες καταστάσεις για τον ορισμό του DPO

2.2.1. Υποχρεωτικός διορισμός βάσει της νομοθεσίας της ΕΕ / των κρατών μελών

Σύμφωνα με το άρθρο. 37 παράγραφος 4 του ΓΚΠΔ, η ΕΕ και τα κράτη μέλη έχουν το δικαίωμα να προβλέψουν για άλλες καταστάσεις, στις οποίες ο διορισμός του ΥΠΔ θα πρέπει να είναι υποχρεωτικός. Αυτός ο υποχρεωτικός διορισμός μπορεί να απαιτηθεί από μια ποιοτική ένδειξη (π.χ. για ορισμένες τομεακές δραστηριότητες επεξεργασίας) ή από μία ποσοτική ένδειξη (π.χ. σε περίπτωση που ο οργανισμός επεξεργάζεται τα προσωπικά δεδομένα ορισμένων υποκειμένων δεδομένων). Η Γερμανία, για παράδειγμα, εισήγαγε στην τοπική νομοθεσία για την προστασία των δεδομένων ευρύτερες απαιτήσεις από τον ΓΚΠΔ: (i) εταιρείες που ασκούν επιχειρηματική δραστηριότητα στη Γερμανία και απασχολούν τουλάχιστον 10 άτομα στον τομέα της αυτοματοποιημένης επεξεργασίας θα είναι υποχρεωμένοι να διορίσουν έναν ΥΠΔ · (ii) σε περιπτώσεις αυτοματοποιημένης επεξεργασίας στο πλαίσιο επιχειρηματικών δραστηριοτήτων είτε (1) για το σκοπό μιας μεταβίβασης, (2) ή για σκοπούς ανώνυμης μεταφοράς είτε (3) για σκοπούς έρευνας αγοράς ή κοινής γνώμης, οι επιχειρήσεις πρέπει να ορίσουν έναν υπεύθυνο προστασίας δεδομένων ανεξάρτητα από τον αριθμό των ατόμων που απασχολούνται για την αυτοματοποιημένη επεξεργασία δεδομένων προσωπικού χαρακτήρα[iv].

2.2.2. Εθελούσιος διορισμός

Ο ΓΚΠΔ προβλέπει επίσης τη δυνατότητα εθελούσιου διορισμού ΥΠΔ. Μια τέτοια προσέγγιση μπορεί να είναι εύλογη για οργανισμούς που είναι πρόθυμοι να επιδείξουν συμμόρφωση με τους κανόνες προστασίας δεδομένων και να προωθήσουν τη διαφάνεια και την εμπιστοσύνη. Δεδομένου ότι η δραστηριότητα των Τοπικών Αρχών θα εμπίπτει μάλλον στην πρώτη υποχρεωτική απαίτηση (δημόσια αρχή / οργανισμός), ο εθελοούσιος διορισμός μπορεί να εφαρμοστεί σε ορισμένους οργανισμούς των οποίων το κεφάλαιο ανήκει στον δήμο / το κράτος - π.χ. επιχειρήσεις δημόσιων μεταφορών, δημόσια σχολεία / πανεπιστήμια, δημόσιοι πάροχοι υπηρεσιών κοινής ωφέλειας (παροχή νερού, φυσικού αερίου, ηλεκτρισμού) κ.λπ.

LATVIAN ASSOCIATION OF LOCAL AND REGIONAL GOVERNMENTS
SMA THE EXTENDED ENTERPRISE
SNSPA

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

2.3. Συμβατικές σχέσεις με τον ΥΠΔ

2.3.1. Σύμβαση εργασίας

Ο ΓΚΠΔ προβλέπει ρητά την ευκαιρία να διοριστεί ο ΥΠΔ βάσει σύμβασης εργασίας. Αυτό συνεπάγεται δύο δυνατότητες: (i) να διοριστεί κάποιος που εργάζεται ήδη στον οργανισμό για να συνδυάσει τη λειτουργία του με τα καθήκοντα του ΥΠΔ, ή (ii) να δημιουργηθεί μια νέα θέση εργασίας για τον ΥΠΔ. Η επιλογή μεταξύ αυτών των δύο δυνατοτήτων εξαρτάται πιο πολύ από τη δομή, τον αριθμό των εργαζομένων, τον φόρτο εργασίας, τον τύπο, τον αριθμό των δραστηριοτήτων επεξεργασίας δεδομένων και θα πρέπει να γίνεται κατά περίπτωση. Αν η αντίστοιχη οργάνωση της Τοπικής Αρχής είναι μάλλον μικρή (π.χ. βρίσκεται σε ένα μικρό χωριό με περιορισμένο αριθμό πολιτών των οποίων τα δεδομένα έχουν υποστεί επεξεργασία), μπορεί να είναι λογικό να μην διοριστεί νέο μέλος του προσωπικού, αλλά να ανατεθεί η λειτουργία του ΥΠΔ σε κάποιον που εργάζεται ήδη στον οργανισμό (σε κάθε περίπτωση πρέπει να αποφεύγεται η σύγκρουση συμφερόντων). Αντίθετα, αν η οργάνωση της Τοπικής Αρχής είναι τεράστια και/ή οι καθημερινές της δραστηριότητες σχετίζονται με την επεξεργασία σημαντικών ποσών προσωπικών δεδομένων (ή ευαίσθητων δεδομένων / δεδομένων που σχετίζονται με καταδίκες και ποινικά αδικήματα), η επιλογή να ανοίξει μια νέα θέση για (τουλάχιστον) έναν ΥΠΔ θα ήταν δικαιολογημένη.

2.3.2. Σύμβαση παροχής υπηρεσιών

Ο ΓΚΠΔ δεν υποχρεώνει τους οργανισμούς να διορίζουν τους ΥΠΔ μόνο ως μέλη προσωπικού. Ο κανονισμός προβλέπει ρητώς ότι η λειτουργία του ΥΠΔ μπορεί να ανατίθεται σε εξωτερικό άτομο / οργανισμό βάσει σύμβασης παροχής υπηρεσιών. Το WP29 συνιστά ως μια καλή πρακτική για τις εξωτερικές ομάδες των ΥΠΔ να έχουν διορισμένο έναν επικεφαλής επικοινωνίας και έναν υπεύθυνο που θα ορίζεται στην σύμβαση παροχής υπηρεσιών[v]. Επιπλέον, κάθε μέλος του εξωτερικού οργανισμού προστασίας δεδομένων πρέπει να πληροί όλες τις ισχύουσες απαιτήσεις στο πλαίσιο του ΓΚΠΔ. Η εξωτερική ανάθεση των λειτουργιών της προστασίας δεδομένων των στον εξωτερικό οργανισμό θα μπορούσε επίσης να είναι λογική, δεδομένου ότι ο οργανισμός αυτός θα διαθέτει το απαιτούμενο επίπεδο ειδικών γνώσεων, εμπειρίας και θα διατηρεί τις σχετικές πιστοποιήσεις[vi].

Τέλος, αλλά εξίσου σημαντικό, ανάλογα με τον τοπικό νόμο, η σύναψη σύμβασης παροχής υπηρεσιών με εξωτερικό υπεύθυνο προστασίας δεδομένων ενδέχεται να απαιτεί τη διεξαγωγή ορισμένων τυπικών διαδικασιών (π.χ. βάσει του νόμου περί δημοσίων συμβάσεων).

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

3. ΘΕΣΗ ΤΟΥ ΥΠΔ

3.1. Συμμετοχή σε όλα τα θέματα που σχετίζονται με την προστασία των προσωπικών δεδομένων

Ο ΓΚΠΔ προβλέπει ρητά ότι ο ΥΠΔ πρέπει να συμμετέχει σε όλα τα θέματα που σχετίζονται με την προστασία των προσωπικών δεδομένων στον οργανισμό. Το WP29 θεωρεί τη συμμετοχή του ΥΠΔ (όσον αφορά τις διαβουλεύσεις, τις συμβουλές, τον έλεγχο κ.λπ.) σε κάθε διαδικασία που περιλαμβάνει την επεξεργασία δεδομένων προσωπικού χαρακτήρα από το αρχικότερο δυνατό στάδιο ως ένα από τα εργαλεία για την διασφάλιση του απορρήτου από το σχεδιασμό[vii].

Οι πρακτικές συνέπειες της συμμετοχής του ΥΠΔ στην οργάνωση θα μπορούσαν να περιλαμβάνουν, για παράδειγμα:

- Αναζήτηση συμβουλών κατά τη διεξαγωγή αξιολόγησης του αντικτύπου της προστασίας δεδομένων (DPIA) (άρθρο 35, παρ. 2 του GDPR);
- Συμμετοχή σε συναντήσεις εργασίας (το WP29 καθορίζει τη συμμετοχή στις συνεδριάσεις της ανώτερης και μεσαίας διοίκησης, αλλά στην πράξη, η αλληλεπίδραση του ΥΠΔ με το προσωπικό σε επίπεδο εμπειρογνωμόνων μπορεί να έχει παρόμοια (αν όχι υψηλότερη) προστιθέμενη αξία);
- Αναζήτηση διαβουλεύσεων από τον ΥΠΔ κάθε φορά που πρέπει κάθε φορά που πρέπει να γίνεται επεξεργασία δεδομένων διαχείρισης;
- Αναζήτηση διαβουλεύσεων από τον ΥΠΔ σχετικά με τα μέτρα που πρέπει να ληφθούν σε περίπτωση παραβίασης των δεδομένων.

3.2. Διασφάλιση αναγκαίων πόρων και ανεξαρτησία

Ο ΥΠΔ δεν θα μπορεί να εκτελεί σωστά το έργο του εάν δεν διαθέτει τους απαραίτητους πόρους. Η διοίκηση του οργανισμού είναι επομένως υπεύθυνη να διασφαλίσει ότι ο ΥΠΔ είναι επαρκώς εξασφαλισμένος τουλάχιστον όσον αφορά:

- **Οργανωτικά θέματα:**
  - Οι ΥΠΔ πρέπει να διαθέτουν ομάδα που να τους υποστηρίζουν κατά την εκτέλεση των καθηκόντων τους. Αυτό είναι ιδιαίτερα σημαντικό για μεγαλύτερους οργανισμούς. Ακόμη και ο διορισμός ορισμένων ΥΠΔ μπορεί να είναι η λύση σε ορισμένες περιπτώσεις.
  - Πρόσβαση σε όλες τις άλλες ομάδες του οργανισμού. Οι ΥΠΔ δεν μπορούν να ασκήσουν σωστά τις λειτουργίες τους αν δεν αλληλεπιδρούν σωστά με όλες τις άλλες ομάδες που είναι υπεύθυνες για την επεξεργασία δεδομένων

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

(π.χ. Υπηρεσία Μητρώου και Αρχειοθέτησης Αρχείων, Νομικό Τμήμα, Ανθρώπινο Δυναμικό, Λογιστική, Τμήμα Πληροφορικής κ.λπ.);

- Υπεύθυνοι μόνο για την ανώτατη διοίκηση. Ο ΓΚΠΔ προβλέπει ρητά ότι οι ΥΠΔ πρέπει να είναι υπεύθυνοι μόνο για την ανώτατη διοίκηση του οργανισμού. Για τις Τοπικές Αρχές αυτό μπορεί να είναι π.χ. του δημάρχου, του δημοτικού συμβουλίου, του διευθυντή / προέδρου της αντίστοιχης διοικητικής μονάδας κλπ. Η απαίτηση αυτή είναι πολύ σημαντική για την εξασφάλιση της ανεξαρτησίας των ΥΠΔ. Εάν η σχέση ΥΠΔ με τη διοίκηση ήταν έμμεση (π.χ. μέσω διαμεσολαβητών όπως ο επικεφαλής του Νομικού Τμήματος ή του Τμήματος Ανθρώπινου Δυναμικού), οι ΥΠΔ δεν μπορούσαν να ασκήσουν σωστά το έργο τους, διότι θα βρίσκονται σε κατάσταση όπου οι ΥΠΔ θα είναι υπόλογοι ενώπιον αυτών που κανονικά θα έπρεπε να ελέγχουν.
- Χρόνος εκτέλεσης του έργου. Η απαίτηση αυτή πρέπει να τηρείται ιδίως στις περιπτώσεις όπου ο ΥΠΔ διορίζεται σε μερική απασχόληση ή όπου ο εξωτερικός ΥΠΔ έχει αναλάβει την προστασία δεδομένων εκτός από τις άλλες υποχρεώσεις του[viii]. Το WP29 προβλέπει ως καλή πρακτική την καθιέρωση ενός ποσοστού χρόνου για τη λειτουργία του ΥΠΔ, όπου δεν βασίζεται στην πλήρη απασχόληση.

- **Οικονομικά θέματα**
  - Ο ΥΠΔ πρέπει να διαθέτει τους απαραίτητους οικονομικούς πόρους για την άσκηση των καθηκόντων του. Εάν ο οργανισμός δεν εξασφαλίσει επαρκή προϋπολογισμό για δραστηριότητες προστασίας δεδομένων, θα μπορούσε να τεθεί σε κίνδυνο η ορθή άσκηση των καθηκόντων του ΥΠΔ.
  - Ο ΥΠΔ πρέπει να διαθέτει τις απαραίτητες εγκαταστάσεις και εξοπλισμό (δωμάτια, υπολογιστές, συνδεσιμότητα στο Internet, βάσεις δεδομένων, τεχνικές λύσεις όπως προγράμματα λογισμικού κ.λπ.)
- **Τα ζητήματα της εκπαίδευσης** – το επίπεδο εμπειρογνωμοσύνης του ΥΠΔ πρέπει να αναβαθμίζεται συνεχώς (μέσω μαθημάτων, διασφάλισης νέας λογοτεχνίας κ.λπ.). Δεδομένου ότι η προστασία των δεδομένων είναι ένας πολύ δυναμικός τομέας της ανθρώπινης γνώσης, είναι κατανοητό ότι ο ΥΠΔ πρέπει να είναι ενημερωμένος με τις τελευταίες τάσεις και εξελίξεις προκειμένου να εξασφαλιστεί σωστά το υψηλότερο δυνατό επίπεδο όσον αφορά την προστασία δεδομένων στον οργανισμό και να αντιμετωπίσει τις νέες προκλήσεις όσον αφορά την τεχνολογική και νομική ανάπτυξη.

Σημαντική πτυχή της ανεξαρτησίας του ΥΠΔ είναι η απαγόρευση επιβολής κυρώσεων / πρόκλησης δυσμενών συνεπειών στον ΥΠΔ για την εκτέλεση των καθηκόντων του. Οι

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

δυσμενείς συνέπειες θα μπορούσαν να ποικίλλουν σε ένα ευρύ φάσμα καταστάσεων - από την απόλυση ή άλλο είδος πειθαρχικής ποινής έως την άρνηση από την προαγωγή, την άρνηση των παροχών που έλαβαν οι άλλοι υπάλληλοι κλπ. Αναμένεται ότι τα κράτη μέλη θα εισαγάγουν τροποποιήσεις στην εργατική νομοθεσία τους και θα προβλέπουν την προστασία των ΥΠΔ κατά την απόλυση για το χρονικό διάστημα κατά την άσκηση των καθηκόντων τους και κάποια περίοδο μετά.[4] Ταυτοχρονα, πρέπει να γίνει μια εύλογη παρεμβολή της απαγόρευσης αυτής - ο ΥΠΔ δεν θα μπορούσε να τιμωρηθεί για τη δέουσα εκτέλεση των υπηρεσιών του. Ωστόσο, εάν ο ΥΠΔ δεν διαθέτει τις απαραίτητες γνώσεις και δεξιότητες, διενέργεια πειθαρχικών παραβιάσεων κ.λπ., οι οργανώσεις θα πρέπει να μπορούν να τον απορρίπτουν για όλους τους λόγους απόλυσης που προβλέπονται στην αντίστοιχη εθνική εργατική νομοθεσία.

3.3. Σύγκρουση συμφερόντων

Εάν ο ΥΠΔ ορίζεται βάσει σύμβασης εργασίας, ο διορισμός αυτός δεν πρέπει να έχει ως αποτέλεσμα σύγκρουση συμφερόντων. Μπορεί να προκύψει σύγκρουση συμφερόντων εάν ο ΥΠΔ έχει άλλη λειτουργία εντός του οργανισμού, η οποία καθορίζει τους σκοπούς και τα μέσα επεξεργασίας δεδομένων εντός δεδομένης εσωτερικής διαδικασίας. Με άλλα λόγια, ο υπεύθυνος προστασίας δεδομένων δεν θα μπορούσε να είναι ταυτόχρονα διευθυντής, διευθύνων σύμβουλος, επικεφαλής λειτουργός, επικεφαλής οικονομικός, επικεφαλής ιατρός, επικεφαλής τμήματος μάρκετινγκ, επικεφαλής ανθρώπινων πόρων ή επικεφαλής τμημάτων πληροφορικής [ix]. Επιπλέον, άλλοι ρόλοι που είναι χαμηλότεροι στην οργανωτική δομή θα μπορούσαν να προκαλέσουν σύγκρουση συμφερόντων, εάν αυτές οι θέσεις ή ρόλοι οδηγούν στον καθορισμό των σκοπών και των μέσων επεξεργασίας (π.χ. λογιστής, νομικός σύμβουλος, ειδικός πληροφορικής).

Μια σύγκρουση συμφερόντων μπορεί να προκύψει όχι μόνο σε περίπτωση διορισμού του ΥΠΔ βάσει σύμβασης εργασίας, αλλά και στην περίπτωση εξωτερικού ΥΠΔ. Εάν ζητηθεί από τον ΥΠΔ να εκπροσωπεί τον ελεγκτή ή τον επεξεργαστή ενώπιον των δικαστηρίων σε υποθέσεις που αφορούν ζητήματα προστασίας δεδομένων, θα προέκυπτε σύγκρουση συμφερόντων, διότι ο ελεγκτής και ο επεξεργαστής έχουν αντιφατικά συμφέροντα.

[4] Germany has already introduced protection for the DPO against dismissal or one year after the appointment ends, except for extraordinary termination reasons. See Demmel, A. The New German Federal Data Protection Act, Squire Patton Boggs, URL: <https://www.squirepattonboggs.com/~/media/files/insights/publications/2017/09/the-new-german-federal-data-protection-act/27836--german-federal-data-protection-alert.pdf> (26.03.2018);

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

4. ΚΑΘΗΚΟΝΤΑ ΤΟΥ ΥΠΔ

4.1. Παρακολούθηση

Ένα από τα βασικά καθήκοντα του ΥΠΔ είναι να παρακολουθεί όλες τις δραστηριότητες επεξεργασίας δεδομένων εντός του οργανισμού. Αυτό συνδέεται εγγενώς με τη λήψη / συλλογή πληροφοριών, την εσωτερική ανάλυση των πληροφοριών αυτών και την αποσαφήνιση, συστάσεις και παροχή συμβουλών εντός του οργανισμού. Η λειτουργία παρακολούθησης επικεντρώνεται στις εσωτερικές διαδικασίες εντός του οργανισμού, με αποτέλεσμα να ενημερώνεται και να συμβουλεύεται όχι μόνο τη διοίκηση αλλά και τους τακτικούς υπαλλήλους σε επίπεδο εμπειρογνωμόνων τα καθήκοντα των οποίων σχετίζονται με την επεξεργασία προσωπικών δεδομένων.

4.2. Αξιολόγηση των Επιπτώσεων της Προστασίας Δεδομένων (ΑΕΠΔ)

Ο ΓΚΠΔ προβλέπει ότι ο ΥΠΔ πρέπει να συμμετέχει στην Αξιολόγηση των Επιπτώσεων της Προστασίας Δεδομένων (ΑΕΠΔ) με συμβουλευτικές λειτουργίες. Το WP29 συνιστά ως θέμα καλής πρακτικής να ζητήσει συμβουλές από τον υπεύθυνο προστασίας δεδομένων σε ένα ή περισσότερα από τα ακόλουθα θέματα σχετικά με την εκτίμηση των επιπτώσεων:

- για το εάν θα πρέπει να διεξάγεται μια ΑΕΠΔ γενικά;
- ποια μεθοδολογία πρέπει να ακολουθείται κατά τη διεξαγωγή της;
- εάν θα πρέπει να διεξάγεται εσωτερικά ή να ανατεθεί σε τρίτους;
- ποιες διασφαλίσεις (συμπεριλαμβανομένων τεχνικών και οργανωτικών μέτρων) θα πρέπει να εφαρμοστούν για να μετριάσουν τους κινδύνους για τα δικαιώματα και τα συμφέροντα των υποκειμένων των δεδομένων;
- εάν η εκτίμηση των επιπτώσεων για την προστασία των δεδομένων έχει πραγματοποιηθεί σωστά και εάν τα συμπεράσματά της συμμορφώνονται με τον ΓΚΠΔ[x].

Εάν η διοίκηση του οργανισμού αποφασίσει να αποκλίνει από τις συμβουλές του ΥΠΔ, ως μέρος της αρχής της λογοδοσίας, είναι σκόπιμο να τεκμηριωθεί αυτή η απόφαση και οι σχετικοί λόγοι και να μπορέσει να παρουσιάσει αυτή την τεκμηρίωση στις εποπτικές αρχές σε περίπτωση ελέγχου.

4.3. Σημείο επαφής

Ο ΥΠΔ είναι το κύριο σημείο επαφής και για τα δύο: τις εποπτικές αρχές (άρθρο 39, παρ. 1, στοιχείο "ε" του ΓΚΠΔ) και τα υποκείμενα των δεδομένων (άρθρο 38, παρ. 4 του ΓΚΠΔ) αναφορικά με θέματα που σχετίζονται με την προστασία δεδομένων εντός του οργανισμού. Ως εκ τούτου, είναι εξαιρετικά σημαντικό να κοινοποιηθούν σωστά τα

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

στοιχεία επικοινωνίας του ΥΠΔ στην εποπτική αρχή και στα πρόσωπα στα οποία αναφέρονται τα δεδομένα. Επιπλέον, η απαίτηση για την παροχή των στοιχείων επικοινωνίας του ΥΠΔ είναι ένα από τα στοιχεία της αρχής της διαφάνειας σύμφωνα με το άρθρο. 12, 13 και 14 του ΓΚΠΔ.

Τίποτα στον ΓΚΠΔ αποκλείει στον ΥΠΔ την ευκαιρία να ζητήσει συμβουλές από τις εποπτικές αρχές σχετικά με οποιοδήποτε ζήτημα που σχετίζεται με την προστασία δεδομένων εντός του οργανισμού.

4.4. Τήρηση αρχείων

Παρόλο που η υποχρέωση τήρησης αρχείων των δραστηριοτήτων επεξεργασίας παρέχεται μόνο για τους ελεγκτές και επεξεργαστές και όχι για τους ΥΠΔ, τίποτα στον ΓΚΠΔ δεν εμποδίζει τους οργανισμούς να αναθέτουν αυτό το καθήκον στον ΥΠΔ. Τα καθήκοντα του ΥΠΔ που απαριθμούνται στον ΓΚΠΔ είναι ελαχίστως καθορισμένα, επομένως, οι οργανισμοί είναι ελεύθεροι, κατά την κρίση τους, να αναθέτουν οποιεσδήποτε άλλες εργασίες στον ΥΠΔ. Το WP29 θεωρεί την κατανομή της υποχρέωσης τήρησης αρχείων στον ΥΠΔ, ως ένα από τα εργαλεία που επιτρέπουν στον ΥΠΔ να εκτελεί τα καθήκοντά του για την παρακολούθηση της συμμόρφωσης, ενημερώνοντας και συμβουλεύοντας τον ελεγκτή/ επεξεργαστή[xi]. Καθώς το αρχείο είναι ένα αποτελεσματικό εργαλείο για την εξασφάλιση λογοδοσίας, θα ήταν εύλογο να ανατεθεί αυτή η υποχρέωση στον ΥΠΔ.

5. ΣΥΜΠΕΡΑΣΜΑ ΚΑΙ ΠΡΑΚΤΙΚΕΣ ΣΥΜΒΟΥΛΕΣ

Ο ΥΠΔ είναι ένας από τους βασικούς παράγοντες για την διασφάλιση της συμμόρφωσης με τους νέους κανόνες προστασίας δεδομένων. Η σπουδαιότητα αυτού του ρόλου εξαρτάται σχεδόν από τον ίδιο τον οργανισμό. Εάν ο οργανισμός εμπλέκει σωστά τον ΥΠΔ σε όλα τα θέματα που σχετίζονται με την προστασία των δεδομένων και εξασφαλίζει τους αναγκαίους πόρους για την εκτέλεση των καθηκόντων του, τότε ο ΥΠΔ μπορεί να είναι ένας από τους καθοριστικούς παράγοντες για τη διασφάλιση της συμμόρφωσης και την ενίσχυση της εμπιστοσύνης μεταξύ των κοινωνιών. Εάν όχι, ο ΥΠΔ θα ήταν μάλλον μια παραπλανητική φιγούρα χωρίς πραγματικές λειτουργίες, παρά την τελική διαχείριση της επικοινωνίας σχετικά με την προστασία των δεδομένων, που αυτό δεν είναι η ιδέα αυτού του ρόλου στον ΓΚΠΔ. Οι Τοπικές Αρχές θα πρέπει να ενθαρρυνθούν να ορίσουν ειδικευμένους υπεύθυνους προστασίας δεδομένων, οι οποίοι, λόγω της έλλειψης καλά προετοιμασμένων ατόμων σε επίπεδο ΕΕ, θα μπορούσαν να αποδειχθούν δύσκολη αποστολή. Σε κάθε περίπτωση, τα επόμενα χρόνια θα προκαθορίσουν τον τρόπο με τον οποίο θα εξελιχθεί ο ρόλος του ΥΠΔ και θα ήταν θετικό για την κοινωνία εάν οι Τοπικές

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

Αρχές είναι ένα από τα πρωτοπόρα παραδείγματα όσον αφορά τον καλύτερο τρόπο χρήσης της μορφής του ΥΠΔ.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

6. ΕΞΩΤΕΡΙΚΕΣ ΠΗΓΕΣ & ΔΙΑΔΙΚΤΥΑΚΟΙ ΣΥΝΔΕΣΜΟΙ

Βιβλία

- **Harting, N.** Datenschutz-Grundverordnung: Das neue Datenschutzrecht in der betrieblichen Praxis, Verlag Dr. Otto Schmidt KG, Köln, 2016;
- **Voigt, P., von dem Bussche, A.** The EU General Data Protection Regulation (GDPR) – A Practical Guide, Springer International Publishing (2017);
- **Boardman, R., Mullock, J., Mole, A.** Bird & Bird Guide to General Data Protection Regulation (2016);
- **EU** General Data Protection Regulation (GDPR). An Implementation and Compliance Guide, IT Governance Publishing, Cambridgeshire (2016);

Έγγραφα της ομάδας εργασίας του άρθρου 29

- WP29, Guidelines on Data Protection Officers ('DPOs'), WP 243 rev.01;

Διαδικτυακοί Σύνδεσμοι

- http://europa.eu/rapid/press-release_IP-18-386_en.htm
- https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en
- ….

7. ΠΑΡΑΠΟΜΠΕΣ

[i] Ibid.
[ii] Ibid, p. 6-7.
[iii] Ibid, p. 8.
[iv] Demmel, A. The New German Federal Data Protection Act, Squire Patton Boggs, URL: <https://www.squirepattonboggs.com/~/media/files/insights/publications/2017/09/the-new-german-federal-data-protection-act/27836--german-federal-data-protection-alert.pdf> (26.03.2018);
[v] WP29, Guidelines on Data Protection Officers ('DPOs'), WP 243 rev.01, p. 22-23.
[vi] EU General Data Protection Regulation (GDPR). An Implementation and Compliance Guide, IT Governance Publishing, Cambridgeshire (2016), p. 58.
[vii] WP29, Guidelines on Data Protection Officers ('DPOs'), WP 243 rev.01, p. 13.
[viii] Ibid, p. 14.
[ix] WP29, Guidelines on Data Protection Officers ('DPOs'), WP 243 rev.01, p. 16.
[x] Ibid, p.17.
[xi] WP29, Guidelines on Data Protection Officers ('DPOs'), WP 243 rev.01, p. 19.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

ProLegis

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

ProLegis

Εκτίμηση αντικτύπου σχετικά με την προστασία δεδομένων

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

ProLegis

Contents

1. Νομικό πλαίσιο 3
   1.1. Γενικός Κανονισμός για την Προστασία Δεδομένων (GDPR ή ΓΚΠΔ)..... 3
2. Πότε είναι απαραίτητη μια ΕΑΠΔ? 6
   2.1. Βασικά..... 6
   2.2. Περιπτώσεις στις οποίες η ΕΑΠΔ είναι επιτακτική..... 7
      2.2.1. Περαιτέρω σκέψεις σχετικά με την ανάγκη διενέργειας μιας ΕΑΠΔ 7
      2.2.2. Διενέργεια μιας ΕΑΠΔ για πολλά παρόμοια συστήματα επεξεργασίας δεδομένων 8
      2.2.3. Θετικοί και αρνητικοί κατάλογοι για την ΕΑΠΔ..... 8
   2.3. Χρόνος διενέργειας της ΕΑΠΔ..... 8
   2.4. Επανεξέταση της ΕΑΠΔ 9
   2.5. Διαβούλευση με την αρχή προστασίας δεδομένων σύμφωνα με το άρθρο 36 του ΓΚΠΔ 10
3. Ποιος είναι υπεύθυνος για τη διενέργεια μιας ΕΑΠΔ;..... 10
   3.1. Βάση 10
   3.2. Συμμετοχή στην ΕΑΠΔ..... 11
4. Πώς διενεργείται μια ΕΑΠΔ..... 12
   4.1. Βάση 12
   4.2. Εφαρμογή μιας ΕΑΠΔ 12
   4.3. Ελάχιστο περιεχόμενο μιας ΕΑΠΔ 13
   4.4. Η επεξεργασία ΕΑΠΔ..... 13
   4.5. Συμπερίληψη των υποκειμένων των δεδομένων και των εκπροσώπων τους .. 15
   4.6. Η έκθεση σχετικά με την εφαρμογή εκτίμησης αντικτύπου για την προστασία της ιδιωτικότητας..... 16
5. Συμπεράσματα και πρακτικές συμβουλές..... 19
6. Εξωτερικές πηγές και σύνδεσμοι 19
   6.1. Βιβλία και άρθρα 19
   6.2. Αρχεία Working Party Άρθρου 29..... 20
   6.3. Διαδικτυακοί σύνδεσμοι..... 20

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

1. Νομικό πλαίσιο

1.1. Γενικός Κανονισμός για την Προστασία Δεδομένων (GDPR ή ΓΚΠΔ)

Άρθρο 35

Εκτίμηση αντικτύπου προστασίας δεδομένων

1. Όταν ένα είδος επεξεργασίας, ιδίως με χρήση νέων τεχνολογιών και συνεκτιμώντας τη φύση, το πεδίο εφαρμογής, το πλαίσιο και τους σκοπούς της επεξεργασίας, ενδέχεται να επιφέρει υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων, ο υπεύθυνος επεξεργασίας διενεργεί, πριν από την επεξεργασία, εκτίμηση των επιπτώσεων των σχεδιαζόμενων πράξεων επεξεργασίας στην προστασία δεδομένων προσωπικού χαρακτήρα. Σε μία εκτίμηση μπορεί να εξετάζεται ένα σύνολο παρόμοιων πράξεων επεξεργασίας οι οποίες ενέχουν παρόμοιους υψηλούς κινδύνους.

2. Ο υπεύθυνος επεξεργασίας ζητεί τη γνώμη του υπευθύνου προστασίας δεδομένων, εφόσον έχει οριστεί, κατά τη διενέργεια εκτίμησης αντικτύπου σχετικά με την προστασία δεδομένων.

3. Η αναφερόμενη στην παράγραφο 1 εκτίμηση αντικτύπου σχετικά με την προστασία δεδομένων απαιτείται ιδίως στην περίπτωση:

(α) συστηματικής και εκτενούς αξιολόγησης προσωπικών πτυχών σχετικά με φυσικά πρόσωπα, η οποία βασίζεται σε αυτοματοποιημένη επεξεργασία, περιλαμβανομένης της κατάρτισης προφίλ, και στην οποία βασίζονται αποφάσεις που παράγουν έννομα αποτελέσματα σχετικά με το φυσικό πρόσωπο ή ομοίως επηρεάζουν σημαντικά το φυσικό πρόσωπο,

(β) μεγάλης κλίμακας επεξεργασίας των ειδικών κατηγοριών δεδομένων που αναφέρονται στο άρθρο 9 παράγραφος 1 ή δεδομένων προσωπικού χαρακτήρα που αφορούν ποινικές καταδίκες και αδικήματα που αναφέρονται στο άρθρο 10 ή

(γ) συστηματικής παρακολούθησης δημοσίως προσβάσιμου χώρου σε μεγάλη κλίμακα.

4. Η εποπτική αρχή καταρτίζει και δημοσιοποιεί κατάλογο με τα είδη των πράξεων επεξεργασίας που υπόκεινται στην απαίτηση για διενέργεια εκτίμησης αντικτύπου σχετικά με την προστασία των δεδομένων δυνάμει της παραγράφου 1. Η εποπτική αρχή

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

ανακοινώνει τον εν λόγω κατάλογο στο Συμβούλιο Προστασίας Δεδομένων που αναφέρεται στο άρθρο 68.

5. Η εποπτική αρχή δύναται επίσης να καταρτίζει και να δημοσιοποιεί κατάλογο με τα είδη των πράξεων επεξεργασίας για τα οποία δεν απαιτείται εκτίμηση αντικτύπου σχετικά με την προστασία των δεδομένων. Η εποπτική αρχή ανακοινώνει τον εν λόγω κατάλογο στο Συμβούλιο Προστασίας Δεδομένων.

6. Πριν από την έκδοση των καταλόγων που αναφέρονται στις παραγράφους 4 και 5, η αρμόδια εποπτική αρχή εφαρμόζει τον μηχανισμό συνεκτικότητας που αναφέρεται στο άρθρο 63, εάν οι εν λόγω κατάλογοι περιλαμβάνουν δραστηριότητες επεξεργασίας οι οποίες σχετίζονται με την προσφορά αγαθών ή υπηρεσιών σε υποκείμενα των δεδομένων ή με την παρακολούθηση της συμπεριφοράς τους σε περισσότερα του ενός κράτη μέλη ή οι οποίες ενδέχεται να επηρεάζουν σημαντικά την ελεύθερη κυκλοφορία των δεδομένων προσωπικού χαρακτήρα στην Ένωση.

7. Η εκτίμηση περιέχει τουλάχιστον:

(α) συστηματική περιγραφή των προβλεπόμενων πράξεων επεξεργασίας και των σκοπών της επεξεργασίας, περιλαμβανομένου, κατά περίπτωση, του έννομου συμφέροντος που επιδιώκει ο υπεύθυνος επεξεργασίας,

(β) εκτίμηση της αναγκαιότητας και της αναλογικότητας των πράξεων επεξεργασίας σε συνάρτηση με τους σκοπούς,

(γ) εκτίμηση των κινδύνων για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων που αναφέρονται στην παράγραφο 1 και

(δ) τα προβλεπόμενα μέτρα αντιμετώπισης των κινδύνων, περιλαμβανομένων των εγγυήσεων, των μέτρων και μηχανισμών ασφάλειας, ώστε να διασφαλίζεται η προστασία των δεδομένων προσωπικού χαρακτήρα και να αποδεικνύεται η συμμόρφωση προς τον παρόντα κανονισμό, λαμβάνοντας υπόψη τα δικαιώματα και τα έννομα συμφέροντα των υποκειμένων των δεδομένων και άλλων ενδιαφερόμενων προσώπων.

8. Η συμμόρφωση με εγκεκριμένους κώδικες δεοντολογίας που αναφέρονται στο άρθρο 40 από τους σχετικούς υπευθύνους επεξεργασίας ή εκτελούντες την επεξεργασία λαμβάνεται δεόντως υπόψη κατά την εκτίμηση του αντικτύπου των πράξεων επεξεργασίας που εκτελούνται από τους εν λόγω υπευθύνους ή εκτελούντες την επεξεργασία, ιδίως για τους σκοπούς εκτίμησης αντικτύπου σχετικά με την προστασία δεδομένων.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

9. Όπου ενδείκνυται, ο υπεύθυνος επεξεργασίας ζητεί τη γνώμη των υποκειμένων των δεδομένων ή των εκπροσώπων τους για τη σχεδιαζόμενη επεξεργασία, με την επιφύλαξη της προστασίας εμπορικών ή δημόσιων συμφερόντων ή της ασφάλειας των πράξεων επεξεργασίας.

10. Όταν η επεξεργασία δυνάμει του άρθρου 6 παράγραφος 1 (γ) ή (ε) έχει νομική βάση στο δίκαιο της Ένωσης ή στο δίκαιο του κράτους μέλους στο οποίο υπόκειται ο υπεύθυνος επεξεργασίας, το εν λόγω δίκαιο ρυθμίζει την εκάστοτε συγκεκριμένη πράξη επεξεργασίας ή σειρά πράξεων και έχει διενεργηθεί ήδη εκτίμηση αντικτύπου σχετικά με την προστασία δεδομένων ως μέρος γενικής εκτίμησης αντικτύπου στο πλαίσιο της έγκρισης της εν λόγω νομικής βάσης, οι παράγραφοι 1 έως 7 δεν εφαρμόζονται, εκτός εάν τα κράτη μέλη κρίνουν απαραίτητη τη διενέργεια της εν λόγω εκτίμησης πριν από τις δραστηριότητες επεξεργασίας.

11. Όπου απαιτείται, ο υπεύθυνος επεξεργασίας προβαίνει σε επανεξέταση για να εκτιμήσει εάν η επεξεργασία των δεδομένων προσωπικού χαρακτήρα διενεργείται σύμφωνα με την εκτίμηση αντικτύπου στην προστασία δεδομένων τουλάχιστον όταν μεταβάλλεται ο κίνδυνος που θέτουν οι πράξεις επεξεργασίας.

Αιτιολογικές εκθέσεις 89 έως 96:

Το άρθρο 35 του ΓΚΠΔ συνδέεται στενά με τα άρθρα 24, 25 και 32. Η κύρια διαφορά μεταξύ του άρθρου 32 και του άρθρου 35 είναι ότι το άρθρο 32 (ασφάλεια επεξεργασίας δεδομένων) εστιάζει στους κινδύνους που συνδέονται με επιζήμια γεγονότα όπως επιθέσεις, ενώ μια εκτίμηση αντικτύπου σχετικά με την προστασία δεδομένων (ΕΑΠΔ) με βάση το άρθρο 35 επικεντρώνεται κυρίως στους κινδύνους που προκύπτουν από την τακτική επεξεργασία δεδομένων.

Η ΕΑΠΔ αποτελεί σημαντικό εργαλείο για την εφαρμογή της προστασίας των δεδομένων με τεχνολογικά μέσα (προστασία δεδομένων κατά το σχεδιασμό), όπως ορίζεται στο άρθρο 25, παράγραφος 1. Και τα δύο βασίζονται στην αρχή της προφύλαξης, δηλαδή στον εντοπισμό κινδύνων ήδη από τις αρχικές φάσεις σχεδιασμού και στην εξέταση σχετικών αντιμέτρων πριν από την εφαρμογή και έναρξη λειτουργίας οποιωνδήποτε συστημάτων επεξεργασίας δεδομένων.

Η ΕΑΠΔ είναι ένα εργαλείο για τον εντοπισμό και την ανάλυση ανάλογων κινδύνων. Στις περιπτώσεις όπου δεν είναι υποχρεωτική μια ΕΑΠΔ, μια ανάλυση των σχετικών κινδύνων είναι απαραίτητη, για την επαρκή εφαρμογή του άρθρου 25 και του άρθρου 32. Και οι δύο κανονισμοί αναφέρονται ρητά στα δικαιώματα και τις ελευθερίες των φυσικών προσώπων. Το βάθος και η απαιτούμενη τεκμηρίωση της ανάλυσης κινδύνου που πρέπει

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

να διεξαχθεί εξαρτάται από την πολυπλοκότητα και την επικινδυνότητα της επεξεργασίας. Συνιστάται η παροχή μιας γραπτής τεκμηρίωσης της ανάλυσης κινδύνου.

Η εφαρμογή της αρχής της προστασίας δεδομένων κατά τον σχεδιασμό υπερβαίνει τους κινδύνους που εντοπίζονται εκ των προτέρων σε μια ανάλυση κινδύνου τελευταίας τεχνολογίας και περιλαμβάνει αποφάσεις που λαμβάνονται σε μεταγενέστερο στάδιο ad hoc (αυθαίρετα) από τους προγραμματιστές συστημάτων (τεχνική διασφάλισης ιδιωτικότητας) κατά την εφαρμογή των αρχών της ελαχιστοποίησης των δεδομένων.

2. Πότε είναι απαραίτητη μια ΕΑΠΔ[1]?

2.1. Βασικά

Μια ΕΑΠΔ πρέπει να εκτελείται πριν από την επεξεργασία δεδομένων προσωπικού χαρακτήρα που φέρουν υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων.

Κατ 'αρχήν, η ΕΑΠΔ πρέπει να διεξάγεται για κάθε μορφή επεξεργασίας δεδομένων, εκτός εάν μπορεί να καθοριστεί εκ των προτέρων ότι τα δικαιώματα και οι ελευθερίες των φυσικών προσώπων δεν επηρεάζονται από μια συγκεκριμένη ενέργεια επεξεργασίας δεδομένων.

Για ποια μορφή επεξεργασίας δεδομένων ένας τέτοιος κίνδυνος πρέπει να υποτεθεί καθορίζεται π.χ. στα σημεία που απαριθμούνται στο άρθρο 35, παράγραφος 3 ή στην αιτιολογική σκέψη 91. Η έμφαση δίδεται στη χρήση των λεγομένων νέων τεχνολογιών, μιας αόριστης νομικής έννοιας που εισήχθη στον ΓΚΠΔ όσον αφορά στην ΕΑΠΔ. Η εκτίμηση κινδύνου όχι μόνο πρέπει να εξετάσει τους υπάρχοντες σχηματισμούς κινδύνου, αλλά και την πιθανότητα μελλοντικών συμβάντων, να προσδιοριστεί σε μια προγνωστική εκτίμηση. Τα αποτελέσματα της εκτίμησης πρέπει να τεκμηριώνονται.

Η τελευταία φράση του άρθρου 35 παράγραφος 1 σε συνδυασμό με την αιτιολογική έκθεση 92 παρέχει μια σημαντική οπτική για την εκτίμηση της ανάγκης μιας ΕΑΠΔ: "Υπάρχουν περιπτώσεις στις οποίες μπορεί να είναι λογικό και οικονομικά σκόπιμο το αντικείμενο μιας εκτίμησης αντικτύπου να μην εφαρμόζεται αποκλειστικά σε ένα συγκεκριμένο έργο, αλλά να διευρύνεται το θεματικό πεδίο εφαρμογής του, για παράδειγμα, εάν δημόσιες αρχές ή δημόσιοι φορείς σκοπεύουν να εγκαθιδρύσουν μια κοινή εφαρμογή ή περιβάλλον επεξεργασίας ή εάν πολλοί ενδιαφερόμενοι φορείς

[1] The following text ist strongly based on the Publication in German Language of Kastelitz, M., Hötzendorfer, W., Riedl, R., Ausgewählte Fragen der Durchführung einer Datenschutz-Folgenabschätzung gemäß Art 35 DSGVO, Jahrbuch Datenschutzrecht 2017, 113ff.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

σχεδιάζουν να θεσπίσουν μια κοινή εφαρμογή ή ένα περιβάλλον επεξεργασίας σε έναν επιχειρηματικό τομέα ή κλάδο, ή για μια ευρέως χρησιμοποιούμενη οριζόντια δραστηριότητα.

2.2. Περιπτώσεις στις οποίες η ΕΑΠΔ είναι επιτακτική

Το άρθρο 35 παρ. 3 απαριθμεί τις υποχρεωτικές περιπτώσεις για μια ΕΑΠΔ:

(a) συστηματική και εκτενής αξιολόγηση προσωπικών πτυχών σχετικά με φυσικά πρόσωπα, η οποία βασίζεται σε αυτοματοποιημένη επεξεργασία, συμπεριλαμβανομένης της κατάρτισης προφίλ και στην οποία βασίζονται αποφάσεις που παράγουν έννομα αποτελέσματα σχετικά με το φυσικό πρόσωπο ή ομοίως επηρεάζουν σημαντικά το φυσικό πρόσωπο ·

(b) μεγάλης κλίμακας επεξεργασία των ειδικών κατηγοριών δεδομένων που αναφέρονται στο άρθρο 9 παράγραφος 1 ή δεδομένων προσωπικού χαρακτήρα που αφορούν ποινικές καταδίκες και αδικήματα που αναφέρονται στο άρθρο 10 ·

(c) συστηματική παρακολούθηση ενός δημοσίως προσβάσιμου χώρου σε μεγάλη κλίμακα.

2.2.1. Περαιτέρω σκέψεις σχετικά με την ανάγκη διενέργειας μιας ΕΑΠΔ

Η αιτιολογική έκθεση 91 απαριθμεί περαιτέρω υποθέσεις που απαιτούν μια ΕΑΠΔ:

Πράξεις επεξεργασίας

(α) οι οποίες ενδέχεται να περιλαμβάνουν μεγάλο αριθμό ατόμων, ή / και υψηλό επίπεδο κινδύνου ή / και χρήση τεχνολογίας ευρείας κλίμακας σύμφωνα με τις σύγχρονες τεχνολογίες ·

(β) οι οποίες συνεπάγονται υψηλό επίπεδο κινδύνου και δυσχεραίνουν τα υποκείμενα των δεδομένων στην άσκηση των δικαιωμάτων τους ·

(γ) στις οποίες δεδομένα προσωπικού χαρακτήρα υποβάλλονται σε επεξεργασία ενόψει της λήψης αποφάσεων σχετικά με συγκεκριμένα φυσικά πρόσωπα έπειτα από οποιαδήποτε συστηματική και εκτενή αξιολόγηση των προσωπικών πτυχών που αφορούν φυσικά πρόσωπα, και βασίζονται στην κατάρτιση προφίλ βάσει των εν λόγω δεδομένων ή έπειτα από επεξεργασία συγκεκριμένων κατηγοριών προσωπικών δεδομένων, βιομετρικών δεδομένων ή δεδομένων που αφορούν ποινικές καταδίκες και αδικήματα ή συναφή μέτρα ασφαλείας ·

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

(δ) οι οποίες συνεπάγονται υψηλό επίπεδο κινδύνου, διότι εμποδίζουν τα υποκείμενα των δεδομένων να ασκήσουν κάποιο δικαίωμα ή να χρησιμοποιήσουν μια υπηρεσία ή σύμβαση ·

(ε) οι οποίες παρουσιάζουν υψηλό κίνδυνο επειδή πραγματοποιούνται συστηματικά σε μεγάλη κλίμακα.

2.2.2. Διενέργεια μιας ΕΑΠΔ για πολλά παρόμοια συστήματα επεξεργασίας δεδομένων

Το άρθρο 35 παρ. 1 δηλώνει ότι μία και μόνο ΕΑΠΔ μπορεί να διενεργείται για συστήματα επεξεργασίας με παρόμοιο επίπεδο κινδύνου. Κατά την εκτίμηση ανάλογων περιπτώσεων πρέπει να λαμβάνεται υπόψη ο συνολικός σκοπός της επεξεργασίας δεδομένων σε κάθε μεμονωμένη περίπτωση. Η αιτιολογική έκθεση 92 αναφέρει ότι, λαμβάνοντας υπόψη το οικονομικό κόστος, η ΕΑΠΔ μπορεί να έχει ένα ευρύτερο θεματικό πεδίο, παρέχοντας στα μέλη σε συγκεκριμένο τομέα ή κλάδο την ευκαιρία να καλύψουν εφαρμογές ή περιβάλλοντα επεξεργασίας ή ευρέως χρησιμοποιούμενες οριζόντιες δραστηριότητες με μια ενιαία ατομική ΕΑΠΔ.

2.2.3. Θετικοί και αρνητικοί κατάλογοι για την ΕΑΠΔ

Μπορεί να υποτεθεί ότι οι εποπτικές αρχές θα δημοσιεύσουν θετικούς / αρνητικούς καταλόγους για να καθοδηγήσουν την απόφαση σχετικά με το εάν απαιτείται μια ΕΑΠΔ σε μια συγκεκριμένη περίπτωση. Οι κατάλογοι αυτοί θα καθορίσουν μορφές επεξεργασίας που απαιτούν ΕΑΠΔ («θετικοί κατάλογοι») και περιπτώσεις όπου δεν απαιτείται ΕΑΠΔ («αρνητικοί»). Οι δύο κατάλογοι πρέπει να διαβιβάζονται από τα εθνικά εποπτικές αρχές στο Ευρωπαϊκό Συμβούλιο για την προστασία των δεδομένων, στο πλαίσιο του καθεστώτος συνοχής των κανονιστικών ρυθμίσεων (άρθρο 35, παρ. 4), ώστε να επιτευχθεί καλύτερη εναρμόνιση σε ολόκληρη την ΕΕ.

Πρέπει να σημειωθεί ότι η ομάδα εργασίας του άρθρου 29 (WP29) συνιστά τη διενέργεια μιας ΕΑΠΔ και στις περιπτώσεις, όπου δεν καθίσταται σαφές αν απαιτείται ΕΑΠΔ ώστε να συμβάλει στην εκπλήρωση των νομικών απαιτήσεων για την ορθή προστασία των δεδομένων.

2.3. Χρόνος διενέργειας της ΕΑΠΔ

Ο χρόνος και η μέθοδος εφαρμογής μιας ΕΑΠΔ οφείλουν να καθορίζονται από τον υπεύθυνο επεξεργασίας. Προβλέπονται νομικές κυρώσεις για την αδυναμία εκτέλεσης μιας ΕΑΠΔ. Συνιστάται να ξεκινά η προετοιμασία για την ΕΑΠΔ κατά το πιο πρώιμο δυνατό στάδιο ενός έργου. Κάθε τμήμα ή τα σχετικά μέλη του προσωπικού που εμπλέκονται στην επεξεργασία δεδομένων πρέπει να ξεκινήσουν τις σχετικές διαδικασίες. Προτείνεται κατάρτιση για την ευαισθητοποίηση σχετικά με την ανάγκη για ΕΑΠΔ στο πλαίσιο του οργανισμού.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

Η λήψη μέτρων για την ελαχιστοποίηση του κινδύνου σε πρώιμο στάδιο κάθε έργου, που περιλαμβάνει την επεξεργασία δεδομένων, μπορεί να συμβάλει στη διατήρηση των γραφειοκρατικών προσπαθειών σε σχετικά χαμηλό επίπεδο.

Μια ΕΑΠΔ μπορεί να καθοδηγήσει την αναζήτηση κατάλληλων λύσεων και να συμβάλει στην αποτελεσματική και έγκαιρη εφαρμογή των απαιτήσεων προστασίας δεδομένων - όπως προαναφέρθηκε- μέσω κατάλληλων τεχνολογικών λύσεων (προστασία δεδομένων κατά το σχεδιασμό) και της επιλογής προεπιλεγμένων ρυθμίσεων για την προστασία των δεδομένων.

Παρέχοντας ολοκληρωμένες και εντατικές προετοιμασίες, η ΕΑΠΔ θα καθοδηγήσει ένα σχεδιαζόμενο πρόγραμμα από το στάδιο των αρχικών ιδεών μέχρι την τελική επιχειρησιακή εφαρμογή του και αποδεικνύει τον επαναληπτικό χαρακτήρα της διαδικασίας ΕΑΠΔ.

Το αν μια ΕΑΠΔ απαιτήθηκε για πράξεις επεξεργασίας που έλαβαν χώρα πριν από τη γενική εφαρμογή του ΓΚΠΔ (25 Μαΐου 2018) συνιστά ανοικτό ερώτημα. Λαμβάνοντας υπόψη την κυριολεκτική διατύπωση («πριν από»), απαιτείται μια ΕΑΠΔ μόνο για τις πράξεις που άρχισαν μετά τις 25 Μαΐου 2018 ή που υφίστανται σημαντικές μεταβολές μετά την ημερομηνία αυτή.

Δεδομένου ότι σε αυτές τις περιπτώσεις το σύστημα επεξεργασίας δεδομένων λειτουργεί ήδη, δεν είναι δυνατός ο προκαταρκτικός έλεγχος. Επιπλέον, αυτές οι ενέργειες δεν υπάρχουν σε ένα μη καθοριζόμενο χώρο (αν υποτεθεί ότι έχουν ληφθεί υπόψη όλοι οι νομικοί κανονισμοί και οι απαιτήσεις υποβολής εκθέσεων του προηγουμένου νομικού πλαισίου).

Παρόλα αυτά, η Ομάδα Εργασίας 29 συνιστά θερμά την εφαρμογή της ΕΑΠΔ για συστήματα επεξεργασίας που ήδη τελούν εν λειτουργία, προκειμένου να αποφευχθούν νομικές ανακρίβειες και ακόμη και νομικές κυρώσεις.

2.4. Επανεξέταση της ΕΑΠΔ

Μετά τη διενέργεια μιας ΕΑΠΔ, η εφαρμογή των προτεινόμενων μέτρων πρέπει να επανεξετασθεί, εάν κρίνεται απαραίτητο. Ενδέχεται να είναι αναγκαία η επανεξέταση της επεξεργασίας δεδομένων για τον εντοπισμό τυχόν νέων στοιχείων των κινδύνων που σχετίζονται με την επεξεργασία των δεδομένων. Η αιτιολογική έκθεση 89 αναφέρει ότι μπορεί να χρειαστεί μια αναθεώρηση της ΕΑΠΔ σε εύθετο χρόνο μετά από μια πρώτη εκτίμηση. Κατά τη διενέργεια μιας ΕΑΠΔ, ένα χρονικό πλαίσιο για ελέγχους ρουτίνας ή μελλοντικές ανανεώσεις πρέπει να συμπεριληφθεί στην τεκμηρίωση.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

Οι τεχνολογικές εξελίξεις, η νέα νομοθετική ρύθμιση και οι αλλαγές στις ρουτίνες επεξεργασίας πρέπει να εξεταστούν. Εάν προκύψει κίνδυνος, πρέπει να διενεργηθεί μια νέα ΕΑΠΔ.

Το καθήκον διενέργειας μια ΕΑΠΔ αποτελεί μέρος των υποχρεώσεων του υπευθύνου επεξεργασίας δεδομένων, που τεκμηριώνει τη λογοδοσία τους. Η τεκμηρίωση και η έκθεση δε θα πρέπει να παρέχουν μόνο πληροφορίες σχετικά με την ΕΑΠΔ που διενεργήθηκε αλλά επίσης να αναφέρουν τους λόγους για τους οποίους δε διενεργήθηκε μια πλήρης ΕΑΠΔ ή τερματίστηκε μια ΕΑΠΔ αφού εντοπίστηκαν υψηλοί κίνδυνοι για τα υποκείμενα των δεδομένων.

2.5. Διαβούλευση με την αρχή προστασίας δεδομένων σύμφωνα με το άρθρο 36 του ΓΚΠΔ

Ο υπεύθυνος της επεξεργασίας δεδομένων πρέπει να συμβουλευθεί την Αρχή Προστασίας Δεδομένων (DPA) σε περίπτωση που η ΕΑΠΔ αποκαλύπτει σημαντικούς κινδύνους και ο υπεύθυνος επεξεργασίας δε γνωρίζει τον τρόπο με τον οποίο μπορεί να λάβει οποιαδήποτε διορθωτικά μέτρα για τον μετριασμό των εν λόγω κινδύνων. Η ΑΠΔ οφείλει να απαντήσει σε αυτή την αίτηση διαβούλευσης εντός δεκατεσσάρων εβδομάδων. Για σύνθετα και καινοτόμα έργα, συνιστάται να ξεκινήσει μια ΕΑΠΔ το συντομότερο δυνατό, ώστε οποιαδήποτε πρόταση της ΑΠΔ να μπορεί να εξεταστεί κατά την εφαρμογή του σχεδίου του έργου.

3. Ποιος είναι υπεύθυνος για τη διενέργεια μιας ΕΑΠΔ;

3.1. Βάση

Η ευθύνη για τη διεξαγωγή μιας ΕΑΠΔ είναι του υπευθύνου επεξεργασίας- στην περίπτωση αυτή της τοπικής δημόσιας αρχής. Αρχικά, η πρόταση της Επιτροπής ανέθετε την ευθύνη για την ΕΑΠΔ στον εκτελούντα την επεξεργασία δεδομένων που ενεργούσε με εντολή του υπευθύνου επεξεργασίας. Αντίθετα, η αιτιολογική έκθεση 95 απλώς απαιτεί από τον εκτελούντα την επεξεργασία να επικουρεί τον υπεύθυνο επεξεργασίας όταν είναι απαραίτητο και κατόπιν αιτήσεως, στη διασφάλιση της τήρησης των υποχρεώσεων που απορρέουν από την εκτίμηση αντικτύπου σχετικά με την προστασία δεδομένων.

Επομένως, στην πράξη θα είναι σκόπιμο να ζητηθεί συμβατικά από έναν εκτελούντα την επεξεργασία, εάν είναι διαθέσιμος και ήδη επιλεγμένος, να εμπλακεί και να υποστηρίξει ενεργά όλη τη διαδικασία ΕΑΠΔ. Αυτό είναι πέραν του άρθρου 28, παράγραφος 3 (στ), το οποίο προβλέπει ότι η σύμβαση για την επεξεργασία (ή άλλο νομικό όργανο) πρέπει να προβλέπει ότι ο εκτελών την επεξεργασία, λαμβάνοντας υπόψη τη φύση της επεξεργασίας και των πληροφοριών που έχει στη διάθεσή του, θα διασφαλίσει τη

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

συμμόρφωση προς τα άρθρα 32 έως 36. Συχνά, μόνο ο εκτελών την επεξεργασία θα έχει τις απαραίτητες πληροφορίες για να εκτιμήσει τις αντίστοιχες πτυχές της επεξεργασίας. Κατά την εκτίμηση, θα πρέπει να λαμβάνεται υπόψη ο κίνδυνος αποκάλυψης των εμπορικών και επιχειρηματικών απορρήτων. Και πάλι συνιστάται αντίστοιχος συμβατικός κανονισμός. Εάν προβλέπεται επεξεργασία δεδομένων από κοινού, η ΕΑΠΔ, σύμφωνα με το άρθρο 35, παρ. 1, εδάφιο 2, μπορεί επίσης να διενεργείται από έναν από τους υπευθύνους επεξεργασίας - κάτι το οποίο δεν απαλλάσσει τους υπολοίπους υπευθύνους επεξεργασίας από τις ευθύνες.

3.2. Συμμετοχή στην ΕΑΠΔ

Η ΕΑΠΔ πρέπει να οργανώνεται ως έργο και ως εκ τούτου θα πρέπει να εξοπλίζεται με τα απαραίτητα υλικά και ανθρώπινα μέσα από ένα αντίστοιχο υψηλό επίπεδο διοίκησης. Κατά την κατάρτιση της ομάδας του έργου πρέπει να δοθεί ιδιαίτερη προσοχή στην πολυπλοκότητα του έργου, στις απαιτούμενες εξειδικευμένες γνώσεις και στις απαιτούμενες γνώσεις σχετικά με το συγκεκριμένο έργο και το περιβάλλον του. Στην πράξη, μπορούν να συγκεντρωθούν μια ομάδα δικηγόρων, IT staff, CISO, υπεύθυνος προστασίας δεδομένων, το τμήμα που έχει αιτηθεί επεξεργασίας («κάτοχος δεδομένων») κ.λπ.

Ιδιαίτερη προσοχή δίνεται στη διασφάλιση της αποφυγής συγκρούσεων συμφερόντων. Συνεπώς, όσοι θα ασχοληθούν με την επεξεργασία δεδομένων στο μέλλον δε θα πρέπει να θεωρούνται ανεξάρτητοι, αλλά από την άλλη πλευρά μπορούν να παράσχουν πολύτιμες πληροφορίες για τον σχεδιασμό της εκτίμησης αντικτύπου ιδιωτικότητας. Η υλοποίηση μπορεί να γίνει από εσωτερική ομάδα καθώς και από εξωτερικά τρίτα μέρη. Ιδανικά, θα πρέπει να συμμετέχει ένας ανεξάρτητος φορέας.

Ο υπεύθυνος επεξεργασίας οφείλει να ζητήσει τη συμβουλή του Υπευθύνου Προστασίας Δεδομένων. Σύμφωνα με το άρθρο 39, παράγραφος 1 (γ), οι συμβουλές σχετικά με την ΕΑΠΔ και ο έλεγχος της εφαρμογής της περιλαμβάνονται μεταξύ των υποχρεωτικών καθηκόντων του ΥΠΔ, αλλά μόνο κατόπιν αιτήματος και όχι σε ηγετική θέση.

Συνεπώς, ο υπεύθυνος επεξεργασίας υποχρεούται να λαμβάνει τις συμβουλές του Υπευθύνου Προστασίας Δεδομένων. Το χρονικό σημείο και ο βαθμός στον οποίον ο υπεύθυνος προστασίας δεδομένων πρέπει να συμμετάσχει στη διαδικασία, συνιστούν απόφαση του υπευθύνου επεξεργασίας. Μια μεταγενέστερη επανεξέταση της τελικής έκθεσης θα ήταν επίσης επιθυμητή. Στην πράξη, συνιστάται θερμά η έγκαιρη συμμετοχή του υπευθύνου προστασίας δεδομένων, λόγω της εμπειρίας του.

Ανάλογα με τον οργανισμό του υπευθύνου επεξεργασίας, συνιστάται να εγκρίνεται η ΕΑΠΔ σε επίπεδο διαχείρισης ή από τον αντίστοιχο εξουσιοδοτημένο φορέα.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

4. Πώς διενεργείται μια ΕΑΠΔ

4.1. Βάση

Πρέπει να επισημανθεί ότι ο ΓΚΠΔ δεν προβλέπει συγκεκριμένη μορφή ή συγκεκριμένη μέθοδο για τον σχεδιασμό μιας εκτίμησης αντικτύπου σχετικά με την προστασία δεδομένων, κάτι το οποίο επί του παρόντος συζητείται εντατικά σε εθνικό και ευρωπαϊκό επίπεδο. Η WP 29 δηλώνει ότι μπορούν να χρησιμοποιηθούν διαφορετικές επιλογές σχεδιασμού για να υποστηριχθεί η εφαρμογή των διατάξεων του ΓΚΠΔ και παραπέμπει σε παραδείγματα υφισταμένων (γενικών ή τομεακών) μοντέλων επεξεργασίας ΕΑΠΔ στο παράρτημα 1.[2]

4.2. Εφαρμογή μιας ΕΑΠΔ

Συνεπώς, ο υπεύθυνος επεξεργασίας είναι βασικά ελεύθερος όσον αφορά στον τρόπο διενέργειας της επεξεργασίας ΕΑΠΔ και μπορεί να την προσαρμόσει στις υπάρχουσες εσωτερικές διαδικασίες, υπό την προϋπόθεση ότι η τοπική δημόσια αρχή λαμβάνει υπόψη τις τέσσερις απαιτήσεις που περιέχονται στο άρθρο 35 παράγραφος 7 του ΓΚΠΔ (α) έως (δ) ως ελάχιστες απαιτήσεις μιας ΕΑΠΔ, την οποία περιγράφει λεπτομερέστερα η ομάδα εργασίας του άρθρου 29 και λαμβάνει επιπλέον υπόψη το σημείο "τα ενδιαφερόμενα μέρη εμπλέκονται" (βλ. άρθρο 35 παρ. 2) και την άποψη των υποκειμένων των δεδομένων [βλ. άρθρο 35 παρ. 9]):

(α) στη συστηματική περιγραφή των προβλεπομένων πράξεων επεξεργασίας και των σκοπών της επεξεργασίας, συμπεριλαμβανομένου, κατά περίπτωση, του έννομου συμφέροντος που επιδιώκει ο υπεύθυνος επεξεργασίας,

(β) στην εκτίμηση της αναγκαιότητας και της αναλογικότητας των πράξεων επεξεργασίας σε συνάρτηση με τους σκοπούς,

(γ) στην εκτίμηση των κινδύνων για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων που αναφέρονται στην παράγραφο 1 και

(δ) στα προβλεπόμενα μέτρα για την αντιμετώπιση των κινδύνων, συμπεριλαμβανομένων των εγγυήσεων, των μέτρων ασφαλείας και των μηχανισμών για την προστασία των δεδομένων προσωπικού χαρακτήρα και για την απόδειξη της συμμόρφωσης με τον παρόντα Κανονισμό, λαμβάνοντας υπόψη τα δικαιώματα και τα

2 WP29, WP 248, 15: Different methodologies (see Annex 1 of WP248 for examples of data protection and privacy impact assessment methodologies) could be used to assist in the implementation of the basic requirements set out in the GDPR (Annex 1).

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

έννομα συμφέροντα των υποκειμένων των δεδομένων και άλλων ενδιαφερομένων προσώπων.

4.3. Ελάχιστο περιεχόμενο μιας ΕΑΠΔ

Το άρθρο 35, παρ. 7, (α) έως (δ) του ΓΚΠΔ σε συνδυασμό με τις αιτιολογικές εκθέσεις 84 και 90 ορίζει ως ελάχιστα τα εξής:

α) συστηματική περιγραφή των προβλεπομένων πράξεων επεξεργασίας και των σκοπών της επεξεργασίας, συμπεριλαμβανομένου, κατά περίπτωση, του έννομου συμφέροντος που επιδιώκει ο υπεύθυνος επεξεργασίας ·

β) εκτίμηση της αναγκαιότητας και της αναλογικότητας των διεργασιών επεξεργασίας σε συνάρτηση με τους σκοπούς ·

γ) εκτίμηση των κινδύνων για τα δικαιώματα και τις ελευθερίες των υποκειμένων των δεδομένων που αναφέρονται στην παράγραφο 1 και

δ) τα προβλεπόμενα μέτρα αντιμετώπισης των κινδύνων, συμπεριλαμβανομένων των εγγυήσεων, των μέτρων ασφαλείας και των μηχανισμών για την προστασία των δεδομένων προσωπικού χαρακτήρα και για την απόδειξη της συμμόρφωσης προς τον παρόντα κανονισμό, λαμβάνοντας υπόψη τα δικαιώματα και τα έννομα συμφέροντα των υποκειμένων των δεδομένων και άλλων ενδιαφερομένων προσώπων

Τα σημεία (γ) και (δ) συνιστούν εκφάνσεις της λεγόμενης "προσέγγισης με βάση τον κίνδυνο" του ΓΚΠΔ και αφορούν όχι μόνο στην εφαρμογή της ΕΑΠΔ αλλά και στο πλαίσιο των άρθρων 24, 25 και 32 του ΓΚΠΔ. Με άλλα λόγια, η ΕΑΠΔ είναι ένα συγκεκριμένο παράδειγμα της προσέγγισης που βασίζεται στον κίνδυνο για την επεξεργασία δεδομένων, για τα δεδομένα -εν ολίγοις- που αναμένεται να συνεπάγονται υψηλό κίνδυνο για τα δικαιώματα και τις ελευθερίες των φυσικών προσώπων και ζητεί εκτενέστερη εκτίμηση κινδύνου και θεραπεία. Κατ 'αρχήν, όμως, οποιοσδήποτε άλλος έλεγχος παραδοχής της επεξεργασίας δεδομένων είναι εγγενής σε μια τέτοια εκτίμηση κινδύνου, συμπεριλαμβανομένων των κατάλληλων τεχνικών και οργανωτικών μέτρων που ελαχιστοποιούν τον κίνδυνο, πριν από την εφαρμογή τους (βλέπε μόνο το άρθρο 24 (1) του ΓΚΠΔ).

4.4. Η επεξεργασία ΕΑΠΔ

Η ΕΑΠΔ θα πρέπει να θεωρηθεί ως μια επεξεργασία (όχι μόνο ως μια έκθεση) που οφείλει να ξεκινήσει το συντομότερο δυνατόν προκειμένου να επηρεάσει το σχεδιασμό του αντικειμένου («έργου»). Ως εκ τούτου, η εκτίμηση αντικτύπου διαφέρει επίσης από έναν

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

έλεγχο που αποτιμά ένα έργο εκ των υστέρων και συνήθως έρχεται πολύ αργά για να «απομακρύνει» τις ανάγκες προστασίας δεδομένων που πρέπει να παραγάγει η ΕΑΠΔ.

Υπάρχουν πολλές προτάσεις για την εφαρμογή μιας επεξεργασίας ΕΑΠΔ, οι οποίες κατά τον ένα ή τον άλλο τρόπο είναι παρόμοιες με τα αποτελέσματα της μελέτης PIAF (2012)[3], η οποία απεικόνιζε τις μεθοδολογίες εκτίμησης αντικτύπου σχετικά με την ιδιωτικότητα σε επτά χώρες (συμπεριλαμβανομένης της κατάρτισης συστάσεων «Βέλτιστης Πρακτικής» και βασικών στοιχείων μιας διαδικασίας εκτίμησης αντικτύπου σχετικά με την ιδιωτικότητα) για την Ευρωπαϊκή Επιτροπή, μεταξύ άλλων. Τα ακόλουθα βασικά στοιχεία εντοπίστηκαν:

1. Προσδιορισμός εάν απαιτείται PIA (πρωταρχική ανάλυση).
2. Προσδιορισμός της ομάδας PIA και καθορισμός όρων αναφοράς.
3. Περιγραφή του προτεινόμενου σχεδίου [και προσδιορισμός των ενδιαφερομένων].
4. Ανάλυση των ροών πληροφόρησης και άλλων αντικτύπων σχετικά με την ιδιωτικότητα.
5. Διαβούλευση με τους ενδιαφερομένους.
6. Διαχείριση κινδύνων [Προσδιορισμός κινδύνων και πιθανών λύσεων].
7. Έλεγχος συμμόρφωσης με το νόμο.
8. Διατύπωση συστάσεων.
9. Προετοιμασία και δημοσίευση της έκθεσης [π.χ. στην ιστοσελίδα του οργανισμού].
10. Εφαρμογή των συστάσεων.
11. Εξωτερική επισκόπηση ή / και έλεγχος [τρίτων].
12. Επανεξέταση της PIA εάν το σχετικό έργο αλλάξει [Ενημέρωση της PIA εάν υπάρχουν αλλαγές στο έργο].

Το μοντέλο ΕΑΠΔ για έξυπνα δίκτυα και συστήματα έξυπνης μέτρησης, το οποίο αναφέρεται ρητώς στη σύσταση 2014/724/ΕΕ της Ευρωπαϊκής Επιτροπής, προβλέπει τα ακόλουθα βήματα:[4]

1. Βήμα 1 Προ-αξιολόγηση και κριτήρια που καθορίζουν την ανάγκη διενέργειας μιας ΕΑΠΔ.
2. Βήμα 2 Έναρξη.

[3] *De Hert/Kloza/Wright* (Hrsg), PIAF, Recommendations for a privacy impact assessment framework for the European Union, Deliverable D3 (2012), http://piafproject.eu/ref/PIAF_D3_final.pdf; more available at http://piafproject.eu/Deliverables.html.

4 Commission Recommendation 2014/724/EU of 10 October 2014 on the Data Protection Impact Assessment Template for Smart Grid and Smart Metering Systems, ABl L 2014/300, 63.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

3. Βήμα 3: Προσδιορισμός, χαρακτηρισμός και περιγραφή των συστημάτων έξυπνου δικτύου / εφαρμογών που επεξεργάζονται προσωπικά δεδομένα.
4. Βήμα 4: Προσδιορισμός των σχετικών κινδύνων.
5. Βήμα 5 Εκτίμηση κινδύνου σχετικά με την προστασία δεδομένων.
6. Βήμα 6 Προσδιορισμός και σύσταση ελέγχων και υπολειπόμενοι κίνδυνοι
7. Βήμα 7 Τεκμηρίωση και σύνταξη της έκθεσης ΕΑΠΔ.
8. Βήμα 8 Επισκόπηση και συντήρηση.

Το νέο πρότυπο ISO / IEC 29134 παρέχει κατευθυντήριες γραμμές για μια διαδικασία διενέργειας αντικτύπου σχετικά με την ιδιωτικότητα και για τη δομή και το περιεχόμενο μιας έκθεσης PIA. Η διαδικασία χωρίζεται στις ακόλουθες τέσσερις υπο-κατηγορίες:

1. Πρωταρχική ανάλυση.
2. Προετοιμασία της PIA.
3. Εκτέλεση του PIA.
4. Επικαιροποίηση της PIA.

Σε ποια και σε πόσα μέρη χωρίζεται μια διαδικασία ΕΑΠΔ είναι μάλλον θέμα προτίμησης, περαιτέρω προτάσεις κυμαίνονται για παράδειγμα από τρεις ή τέσσερις φάσεις σε έξι έως επτά στάδια. Περισσότερο σημαντική είναι η κατανόηση της δομής και η επεξεργασία της διαδικασίας, η οποία λαμβάνει ιδίως υπόψη τις απαιτήσεις του άρθρου 35 (7) του ΓΚΠΔ και τις συστάσεις της Ομάδας Εργασίας του άρθρου 29.

4.5. Συμπερίληψη των υποκειμένων των δεδομένων και των εκπροσώπων τους

Σύμφωνα με το άρθρο 35 παράγραφος 9, ο υπεύθυνος επεξεργασίας θα ζητήσει, κατά περίπτωση, τις απόψεις των υποκειμένων των δεδομένων ή των εκπροσώπων τους σχετικά με την προβλεπόμενη διαδικασία, με την επιφύλαξη της προστασίας του εμπορικού ή του δημοσίου συμφέροντος ή της ασφάλειας των διεργασιών επεξεργασίας. Η συμπερίληψη της φράσης «κατά περίπτωση» στο πλαίσιο των τριμερών διαπραγματεύσεων δεν καθιστά σαφείς τις συγκεκριμένες συνθήκες υπό τις οποίες απαιτείται η παρουσία του ενδιαφερομένου ή του εκπροσώπου του και σε ποιες περιπτώσεις (επιτρεπτές) μπορεί αυτή να αγνοηθεί.

Η μορφή με την οποία ζητείται η γνωμοδότηση είναι ασαφής και η WP29 αναγνωρίζει διαφορετικούς τρόπους, όπως τη διεξαγωγή μελέτης (εσωτερικής ή εξωτερικής), επίσημων συνεντεύξεων με εκπροσώπους του προσωπικού ή συνδικάτων και την υποβολή ερωτηματολογίου σε μελλοντικούς πελάτες του υπευθύνου επεξεργασίας. Από την ίδια τη διατύπωση μπορεί να αντληθεί μόνο η άποψη (στην αρχική εκδοχή των

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

κρατών μελών «της γνωμοδότησης»), αλλά όχι η υποχρέωση να λαμβάνεται υπόψη ή ακόμη και μια (νέα) απαίτηση συγκατάθεσης (πέραν του νόμου για τον Κανονισμό Εργασίας / Labour Constitution Act (ArbVG)) του συμβουλίου εργαζομένων ως εκπροσώπου των ενδιαφερομένων. Ο υπεύθυνος επεξεργασίας, ωστόσο, θα πρέπει να ασχοληθεί με τις απόψεις των υποκειμένων των δεδομένων ή των εκπροσώπων τους και θα πρέπει να τις λάβει υπόψη κατά την εκτίμηση αντικτύπου. Το αν οι οργανισμοί προστασίας καταναλωτών μπορούν επίσης να συμπεριληφθούν στον όρο «εκπρόσωπος» είναι αμφιλεγόμενο στη βιβλιογραφία.[5]

Εν πάση περιπτώσει, η υποχρέωση διαβούλευσης με ρητή δήλωση δεν θίγει την προστασία εμπορικών ή δημοσίων συμφερόντων ή την ασφάλεια των πράξεων επεξεργασίας. Συνεπώς, ο υπεύθυνος επεξεργασίας μπορεί να περιορίσει ή να αρνηθεί σε μεγάλο βαθμό την υποχρέωση ενημέρωσης των ενδιαφερομένων προσώπων ή των εκπροσώπων σχετικά με την προβλεπόμενη διαδικασία σύμφωνα με το άρθρο 35 (9) (η οποία, στην τελευταία περίπτωση, θα οδηγήσει στο να μην είναι δυνατή η συμμετοχή εκ των προτέρων υπό την έννοια του άρθρου 35 (9), δεδομένου ότι η ύπαρξη επαρκών πληροφοριών αποτελεί απαραίτητη προϋπόθεση για τη γνώμη των ενδιαφερομένων ή των εκπροσώπων τους).

Για την εφαρμογή της εκτίμησης αντικτύπου σχετικά με την προστασία δεδομένων, συνιστάται να τεκμηριώνεται στην έκθεση για αποδεικτικούς λόγους για ποιο λόγο έχει ληφθεί περιορισμένη άποψη σχετικά με το περιεχόμενο ή δεν έχει ληφθεί καμία ή για ποιο λόγο δεν έχει ληφθεί γνώμη ή έχει ληφθεί και έχει εξεταστεί μόνο εν μέρει.

4.6. Η έκθεση σχετικά με την εφαρμογή εκτίμησης αντικτύπου για την προστασία της ιδιωτικότητας

Θα πρέπει να σημειωθεί σε αυτό το σημείο ότι η έκθεση ΕΑΠΔ δεν είναι ο πραγματικός στόχος μιας ΕΑΠΔ, αλλά ένα «μέσο για τον τελικό σκοπό» , μια τεκμηρίωση της διαδικασίας (εσωτερική και εξωτερική). Η υποβολή εκθέσεων δεν πρέπει να υποτιμάται - τεκμηριώνει την υλοποίηση και τα αποτελέσματα και μια απλή Η "PR DPIA report" πρέπει να αποφεύγεται για λόγους συμμόρφωσης. Η έκθεση μπορεί επίσης να χρησιμεύσει ως οδηγός και κατάλογος ελέγχου κατά τη διενέργεια της ΕΑΠΔ.

Το Άρθρο 35 του ΓΚΠΔ δεν περιέχει, απροσδόκητα κατά κάποιο τρόπο , καμία ρητή απαίτηση για την εκπόνηση έκθεσης σχετικά με τη διενέργεια της ΕΑΠΔ. Ωστόσο, το

5 *Martini* in Paal/Pauly (Hrsg), Datenschutz-Grundverordnung (2016) Art 35 Rz 60; dagegen (mangels rechtlicher Verbundenheit) *Laue/Nink/Kremer*, Das neue Datenschutzrecht in der betrieblichen Praxis (2016) 245 Rz 99.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

γεγονός ότι υπάρχει υποχρέωση τεκμηρίωσης από πλευράς υπευθύνου επεξεργασίας είναι αναμφισβήτητο και ακολουθεί σιωπηρά το άρθρο 35 παρ. 7 του ΓΚΠΔ καθώς και το άρθρο 5 παρ. 2 του ΓΚΠΔ (λογοδοσία) σε συνδυασμό με το άρθρο 24 παρ. 1 του ΓΚΠΔ και το άρθρο 36 (3) (ε) (που απαιτεί από τον επιβλέποντα να παράσχει "την εκτίμηση αντικτύπου προστασίας δεδομένων που αναφέρεται στο άρθρο 35"). Επίσης, η επανεξέταση που απαιτείται από το άρθρο 35 παρ. 11 για να εκτιμηθεί κατά πόσον η επεξεργασία διενεργείται σύμφωνα με την ΕΑΠΔ απαιτεί να διατηρηθούν τα αποτελέσματα της εκτίμησης αντικτύπου. Επιπλέον, η υποβολή εκθέσεων σχετικά με τις ΑΠΔ είναι σύμφωνη με την παγκόσμια ορθή πρακτική σε αυτόν τον τομέα (βλ. Το τμήμα IV.1 κατωτέρω), η οποία βασίζεται στην ΕΑΠΔ που προβλέπεται στο άρθρο 35 του ΓΚΠΔ.

Συνιστάται η συνοδευτική διαδικασία ΕΑΠΔ με τεκμηρίωση υπό την έννοια του «ζωντανού εγγράφου», αρχίζοντας με την τεκμηρίωση της πρωταρχικής ανάλυσης, σε περίπτωση που δεν είναι απαραίτητη η διενέργεια μιας ΕΑΠΔ. Ακόμη και αν αυτή η ανάλυση δείξει ότι δεν απαιτείται ΕΑΠΔ και η διαδικασία ανασταλεί, ο υπεύθυνος επεξεργασίας θα είναι υπεύθυνος για τη λογοδοσία και τα αποδεικτικά στοιχεία της. Η γραπτή αυτή τεκμηρίωση μπορεί να υποβληθεί στον επόπτη σε οποιαδήποτε μελλοντική διαδικασία και θα ανιχνεύει εσωτερικές θεωρήσεις και εκτιμήσεις.

Όσον αφορά στο περιεχόμενο, η έκθεση ΕΑΠΔ καθορίζει ουσιαστικά τη διαδικασία (συμπεριλαμβανομένης της παρουσίασης των γεγονότων με την έννοια της συστηματικής περιγραφής ολόκληρου του αντικειμένου της δοκιμής - «στόχος της αξιολόγησης») και τα αποτελέσματα της διενέργειας ΕΑΠΔ. Όπως και στην περίπτωση της ίδιας της διενέργειας ΕΑΠΔ, ο ΓΚΠΔ δεν προβλέπει ειδικούς κανόνες για το σχεδιασμό μιας έκθεσης ΕΑΠΔ. Ωστόσο, ως ελάχιστο περιεχόμενο, τα κριτήρια που απαριθμούνται στην Ομάδα Εργασίας του Άρθρου 29 για την προστασία δεδομένων στο Παράρτημα 2 WP 248, τα οποία βασίζονται ουσιαστικά στο Άρθρο 35 παρ. 7, είναι προκαθορισμένα. Το ISO / IEC 29134 συνιστά τα ακόλουθα περιεχόμενα της έκθεσης εκτίμησης αντικτύπου σχετικά με την ιδιωτικότητα, με έμφαση στην εκτίμηση των κινδύνων:

1. Σχετικές απαιτήσεις ιδιωτικότητας.
2. Περιγραφή του πεδίου εφαρμογής.
3. Περιγραφή των χρησιμοποιουμένων κριτηρίων κινδύνου.
4. Συμμετέχοντες στην υλοποίηση.
5. Διαβουλεύσεις με τους ενδιαφερομένους.

Αυτό υποστηρίζεται επίσης από την αιτιολογική έκθεση 90, η οποία αναφέρει, μεταξύ άλλων, τα εξής: «Η εκτίμηση αντικτύπου πρέπει να περιλαμβάνει ιδίως τα προβλεπόμενα μέτρα, εγγυήσεις και μηχανισμούς που μετριάζουν αυτόν τον κίνδυνο, διασφαλίζουν την

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

προστασία των δεδομένων προσωπικού χαρακτήρα και αποδεικνύουν τη συμμόρφωση προς τον παρόντα κανονισμό».

Στην αναλυτική μελέτη PIAF, το ελάχιστο περιεχόμενο μιας έκθεσης ΑΠΔ έχει ως εξής: [6]

1. Εισαγωγή και πληροφορίες σχετικά με το ποιος έχει αναλάβει την ΕΑΠΔ, τα στοιχεία επικοινωνίας της και πού θα βρεθούν περισσότερες πληροφορίες και άλλες πηγές βοήθειας και συμβουλών
2. Περιγραφή του έργου, των ροών πληροφοριών και των αντικτύπων σχετικά με την ιδιωτικότητα.
3. Αποτελέσματα της διαβούλευσης με τα ενδιαφερόμενα μέρη.
4. Περιγραφή των φάσεων εκτίμησης κινδύνων και μετριασμού των κινδύνων, συμπεριλαμβανομένων των εναλλακτικών λύσεων που εξετάζονται.
5. Ανάλυση της συμμόρφωσης με το νόμο.
6. Συστάσεις.
7. Παραρτήματα, εάν είναι απαραίτητο.

Εάν είναι διαθέσιμη η έκθεση ή το τελικό σχέδιο, μπορεί να προκύψει το ερώτημα σχετικά με το τι πρέπει να γίνει με τον υπεύθυνο (εσωτερικά), κυρίως εάν και από ποιον πρόκειται να «εγκριθεί» - ένα πρακτικά σημαντικό σημείο το οποίο παραμένει ασαφές στον ΓΚΠΔ. Το ICO ορίζει ρητώς στον Κώδικα Πρακτικής του τα εξής: «να εξασφαλισθεί η κατάλληλη υπογραφή στο πλαίσιο του οργανισμού». Δεδομένου ότι ο υπεύθυνος πρέπει να διενεργήσει την ΕΑΠΔ, προκύπτει ότι οι αρμόδιοι εκπρόσωποι του υπευθύνου προσώπου εμπλέκονται στην ΕΑΠΔ και έχουν επίσης την τελική ευθύνη. Οι υπεύθυνοι διαχείρισης θα έχουν συνήθως την τελική ευθύνη λήψης αποφάσεων σχετικά με το θέμα και τη φύση του έργου ΕΑΠΔ. Ως ελάχιστη παραλλαγή, ο υπεύθυνος διαχείρισης έργου ή υπεύθυνος προστασίας δεδομένων οφείλουν να αναφέρουν στο «ανώτατο επίπεδο διαχείρισης», όπως προβλέπεται στο άρθρο 38 (3) του ΓΚΠΔ.

Ο ΓΚΠΔ δεν έχει καμία υποχρέωση δημοσίευσης της ΕΑΠΔ, αλλά η WP29 συνιστά τη δημοσίευσή της (τουλάχιστον εν μέρει) προκειμένου να αυξηθεί η εμπιστοσύνη στην επεξεργασία δεδομένων και να προωθηθεί η διαφάνεια. Συγκεκριμένα, η δημοσίευση ενθαρρύνεται σε περιπτώσεις όπου ένα μέρος του κοινού θα επηρεαστεί από την (προγραμματισμένη) διαδικασία.

6 *De Hert/Kloza/Wright* (Hrsg), PIAF, Recommendations for a privacy impact assessment framework for the European Union, Deliverable D3 (2012) 31, http://piafproject.eu/ref/PIAF_D3_final.pdf.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

5. Συμπεράσματα και πρακτικές συμβουλές

Ειδικότερα, οι ρυθμιστικοί οργανισμοί με επαρκείς πόρους έχουν αναπτύξει τις δικές τους προσεγγίσεις για την εκτίμηση αντικτύπου σχετικά με την ιδιωτικότητα κατά τη διάρκεια των ετών. Σύμφωνα με την τωρινή προοπτική, αναμένεται ότι οι αρχές προστασίας δεδομένων που έχουν ήδη αναπτύξει το δικό τους μοντέλο θα το προτιμήσουν ή θα το διαδώσουν, κυρίως επειδή η γνώση της αντίστοιχης εποπτικής αρχής σχετικά με τις δικές τους συστάσεις θα είναι πιο σαφής. Το περιεχόμενο των επί του παρόντος διαθέσιμων μοντέλων εθνικών εποπτικών αρχών (από κράτη μέλη της ΕΕ) συχνά προηγείται του ΓΚΠΔ και δεν έχει προσαρμοστεί (ακόμη) συστηματικά στις απαιτήσεις ή την ορολογία του ΓΚΠΔ.

Πάντως, ο ICO πρόσθεσε τον Κώδικα Πρακτικής ΑΠΔ (2014) στην (αξιοπρόσεκτη) έκθεση σχετικά με «μεγάλα δεδομένα, τεχνητή νοημοσύνη, μηχανική μάθηση και προστασία δεδομένων» στις απαιτήσεις και την ορολογία του ΓΚΠΔ, κάτι που αναμένεται και από τις άλλες αρχές προστασίας δεδομένων. Επίσης, αναμένεται να φανεί εάν το Ευρωπαϊκό Συμβούλιο Προστασίας Δεδομένων (Άρθρο 68) θα παράσχει κατευθυντήριες γραμμές, συστάσεις ή / και βέλτιστες πρακτικές για την ΕΑΠΔ σύμφωνα με το Άρθρο 70 (1) (ε).

Συστάσεις με μια ματιά:

- Τεκμηρίωση όλων των αποφάσεων, ιδίως γιατί δεν έχει διενεργηθεί ΕΑΠΔ (εάν είναι εφαρμόσιμη);
- Σε περίπτωση αμφιβολίας, πραγματοποιήστε μια ΕΑΠΔ:
- Συμμετοχή εσωτερικών και εξωτερικών ενδιαφερομένων;
- Χρήση των προτύπων, των βέλτιστων πρακτικών και, ανάλογα με την περίπτωση, των παρόμοιων ΕΑΠΔ που έχουν ήδη τεθεί σε ισχύ
- Δημοσίευση της ΕΑΠΔ:
  - Ειδικά από τις δημόσιες αρχές;
  - Δημιουργεί και αυξάνει την εμπιστοσύνη στην ιδιωτική ζωή;

6. Εξωτερικές πηγές και σύνδεσμοι

6.1. Βιβλία και άρθρα

- ***Kastelitz, M., Hötzendorfer, W., Riedl, R.***, Ausgewählte Fragen der Durchführung einer Datenschutz-Folgenabschätzung gemäß Art 35 DSGVO, Jahrbuch Datenschutzrecht 2017, 113ff.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

- ***De Hert, Paul/Kloza, Dariusz/Wright, David,*** Recommendations for a privacy impact assessment framework for the European Union http://www.piafproject.eu/ref/PIAF_D3_final.pdf
- ***Wright, David/De Hert, Paul* (Ed.),** Privacy Impact Assessment, Springer Science & Business Media, Dordrecht, Heidelberg, London, New York 2012
- ***De Hert/Kloza/Wright*** (Ed.), **PIAF**, Recommendations for a privacy impact assessment framework for the European Union, Deliverable D3 (2012), http://piafproject.eu/ref/PIAF_D3_final.pdf; more available at http://piafproject.eu/Deliverables.html.
- ***Martini in Paal/Pauly*** (Ed.), Datenschutz-Grundverordnung (2016) Art 35 Rz 60; dagegen (mangels rechtlicher Verbundenheit) Laue/Nink/Kremer, Das neue Datenschutzrecht in der betrieblichen Praxis (2016) 245 Rz 99.

6.2. Αρχεία Working Party Άρθρου 29

- Artikel-29-Working Party, WP 248, April 4, 2017: Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679 http://ec.europa.eu/newsroom/document.cfm?doc_id=44137
- WP 248, as last Revised and adopted on 4 October 2017 (rev.01): Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679 https://www.dsb.gv.at/documents/22758/112500/Guidelines_on_Data_Protection_Impact_Assessment_(DPIA).pdf/ed5daa8c-d388-43a6-9842-629b8175a99c

6.3. Διαδικτυακοί σύνδεσμοι

- Brussels Laboratory for Data Protection and Privacy Impact Assessments http://www.vub.ac.be/LSTS/dpialab/
- ICO, Big data, artificial intelligence, machine learning and data protection (2017), 99 f, https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

ProLegis

ΔΙΑΦΑΝΕΙΑ

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

ProLegis

Contents

1. LEGAL FRAMEWORK 4
   1.1. Treaties of the European Union 4
   1.2. Charter of Fundamental Rights of the EU 4
   1.3. GDPR 4
2. THE MEANING OF TRANSPARENCY UNDER GDPR 5
   2.1. Elements of transparency under GDPR (Art. 12) 6
      2.1.1. "Concise, transparent, intelligible and easily accessible" 6
      2.1.2. "Clear and plain language" 6
      2.1.3. Manner of provision of information (art. 12, para 1 & para 5 "free of charge"). 7
   2.2. Information to be provided to the data subjects (Art. 13 & Art. 14) 7
      2.2.1. What information should be provided? 7
      2.2.3 How the information should be provided? 9
      2.2.4. When to provide information? 10
      2.2.5. When to provide notification in case of changes to the transparency information data controllers should provide? 10
   2.3. Modalities 11
      2.3.1. Privacy notices/ statements 11
      2.3.2. "Push" & "pull" notices 11
      2.3.3. Other types of "Appropriate measures" 12
      2.3.4. Visualisation 12
   2.4. Exercise of data subject rights 12
      2.4.1.Exemptions of the obligation to provide information 13
3. CONCLUSION & PRACTICAL ADVICES 13
4. EXTERNAL SOURCES & WEBLINKS 15

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

Books.....**Грешка! Показалецът не е дефиниран.**
Documents of the Article 29 Working Party .....**Грешка! Показалецът не е дефиниран.**
Web Links .....**Грешка! Показалецът не е дефиниран.**
5. REFERENCES 15

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

1. ΝΟΜΙΚΟ ΠΛΑΙΣΙΟ

1.1. Συνθήκες της Ευρωπαϊκής Ένωσης

Άρθρο 1 της ΣΕΕ -> οι αποφάσεις λαμβάνονται "όσο το δυνατόν πιο ανοικτά και όσο το δυνατόν πλησιέστερα στον πολίτη"

Άρθρο 11 παράγραφος 2 της ΣΕΕ -> «Τα θεσμικά όργανα διατηρούν ανοιχτό, διαφανή και τακτικό διάλογο με τις αντιπροσωπευτικές ενώσεις και την κοινωνία των πολιτών».

Άρθρο 15 της ΣΛΕΕ -> οι πολίτες της Ένωσης που έχουν δικαίωμα πρόσβασης σε έγγραφα των θεσμικών και λοιπών οργάνων και οργανισμών της Ένωσης καθώς και στα προαπαιτούμενα θεσμικών και λοιπών οργάνων και οργανισμών της Ένωσης, ώστε να εξασφαλίζεται η διαφάνεια των διαδικασιών τους.

1.2. Χάρτης Θεμελιωδών Δικαιωμάτων της ΕΕ

Η διαφάνεια αποτελεί παράγοντα ζωτικής σημασίας της αρχής της δίκαιης επεξεργασίας. Αυτή η διαφάνεια εμπίπτει στο άρθρο 8 του Χάρτη των Θεμελιωδών Δικαιωμάτων της ΕΕ.

Άρθρο 8

Προστασία των δεδομένων προσωπικού χαρακτήρα

1. Κάθε πρόσωπο έχει δικαίωμα στην προστασία των δεδομένων προσωπικού χαρακτήρα που το αφορούν.

2. Η επεξεργασία αυτών των δεδομένων πρέπει να γίνεται νομίμως, για καθορισμένους σκοπούς και με βάση τη συγκατάθεση του ενδιαφερομένου ή για άλλους θεμιτούς λόγους που προβλέπονται από το νόμο. Κάθε πρόσωπο δικαιούται να έχει πρόσβαση στα συλλεγέντα δεδομένα που το αφορούν και να επιτυγχάνει τη διόρθωσή τους.

3. Ο σεβασμός των κανόνων αυτών υπόκειται στον έλεγχο ανεξάρτητης αρχής.

1.3. ΓΚΠΔ

Αιτιολογική Σκέψη 39

Θα πρέπει να είναι σαφές για τα φυσικά πρόσωπα ότι δεδομένα προσωπικού χαρακτήρα που τα αφορούν συλλέγονται, χρησιμοποιούνται, λαμβάνονται υπόψη ή υποβάλλονται κατ' άλλο τρόπο σε επεξεργασία, καθώς και σε ποιο βαθμό τα δεδομένα προσωπικού χαρακτήρα υποβάλλονται ή θα υποβληθούν σε επεξεργασία. Η αρχή

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

αυτή απαιτεί κάθε πληροφορία και ανακοίνωση σχετικά με την επεξεργασία των εν λόγω δεδομένων προσωπικού χαρακτήρα να είναι εύκολα προσβάσιμη και κατανοητή και να χρησιμοποιεί σαφή και απλή γλώσσα. Αυτή η αρχή αφορά ιδίως την ενημέρωση των υποκειμένων των δεδομένων σχετικά με την ταυτότητα του υπευθύνου επεξεργασίας και τους σκοπούς της επεξεργασίας και την περαιτέρω ενημέρωση ώστε να διασφαλιστεί δίκαιη και διαφανής επεξεργασία σε σχέση με τα εν λόγω φυσικά πρόσωπα και το δικαίωμά τους να λαμβάνουν επιβεβαίωση και να επιτυγχάνουν ανακοίνωση των σχετικών με αυτά δεδομένων προσωπικού χαρακτήρα που υπόκεινται σε επεξεργασία.

Αιτιολογική Σκέψη 58

Η αρχή της διαφάνειας απαιτεί οποιαδήποτε ενημέρωση που απευθύνεται στο κοινό ή στο υποκείμενο των δεδομένων να είναι συνοπτική, εύκολα προσβάσιμη και εύκολα κατανοητή και να χρησιμοποιείται σαφής και απλή διατύπωση και, επιπλέον, κατά περίπτωση, απεικόνιση. Οι πληροφορίες αυτές θα μπορούσαν να παρέχονται σε ηλεκτρονική μορφή, για παράδειγμα, όταν απευθύνονται στο κοινό, μέσω ιστοσελίδας. Αυτό έχει ιδιαίτερη σημασία σε περιπτώσεις στις οποίες η πληθώρα των συμμετεχόντων και η πολυπλοκότητα των χρησιμοποιούμενων τεχνολογιών καθιστούν δύσκολο για το υποκείμενο των δεδομένων να γνωρίζει και να κατανοεί εάν, από ποιον και για ποιο σκοπό συλλέγονται δεδομένα προσωπικού χαρακτήρα που το αφορούν,όπως στην περίπτωση επιγραμμικής διαφήμισης. Δεδομένου ότι τα παιδιά χρήζουν ειδικής προστασίας, κάθε ενημέρωση και ανακοίνωση, εάν η επεξεργασία απευθύνεται σε παιδί, θα πρέπει να διατυπώνεται σε σαφή και απλή γλώσσα την οποία το παιδί να μπορεί να κατανοεί εύκολα.

Άρθρο 5, παράγραφος 1, στοιχείο (α)

Αρχές που διέπουν την επεξεργασία δεδομένων προσωπικού χαρακτήρα

1. Τα δεδομένα προσωπικού χαρακτήρα:

(α) υποβάλλονται σε σύννομη και θεμιτή επεξεργασία με διαφανή τρόπο σε σχέση με το υποκείμενο των δεδομένων («νομιμότητα, αντικειμενικότητα και διαφάνεια»)

2. Η ΕΝΝΟΙΑ ΤΗΣ ΔΙΑΦΑΝΕΙΑΣ ΣΤΟ ΠΛΑΙΣΙΟ ΤΟΥ ΓΚΠΔ

Η αρχή της διαφάνειας συνδέεται με τις αρχές της δικαιοσύνης και της λογοδοσίας. Το άρθρο 5 (Αρχές που διέπουν την επεξεργασία δεδομένων προσωπικού χαρακτήρα)

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

υποχρεώνει τους ελεγκτές να αποδεικνύουν ότι τα δεδομένα προσωπικού χαρακτήρα διεκπεραιώνονται κατά τρόπο διαφανή. Σύμφωνα με την ομάδα εργασίας του άρθρου 29 (WP29)[i], για την προστασία των δεδομένων, η διαφάνεια στοχεύει στην ενδυνάμωση των υποκειμένων των δεδομένων να κρατήσουν τους επεξεργαστές και ελεγκτές δεδομένων υπεύθυνους και στο να ασκούν έλεγχο επί των προσωπικών τους δεδομένων[ii]. Ο στόχος αυτός επιτυγχάνεται με την εισαγωγή συγκεκριμένων πρακτικών απαιτήσεων, οι οποίες θα πρέπει να τηρούνται σε όλα τα στάδια της επεξεργασίας: πριν ή κατά την έναρξη της επεξεργασίας των δεδομένων, κατά τη συλλογή των προσωπικών δεδομένων και καθ 'όλη την περίοδο επεξεργασίας.

2.1. Στοιχεία διαφάνειας βάσει του ΓΚΠΔ (άρθρο 12)

2.1.1. "Συνοπτική, διαφανής, κατανοητή και εύκολα προσβάσιμη"

Τα πρώτα δύο μέρη αυτής της απαίτησης σημαίνουν ότι οι ελεγκτές δεδομένων πρέπει να παρουσιάζουν τις πληροφορίες / επικοινωνία αποτελεσματικά και με σύντομο τρόπο για να αποφευχθεί η πληροφοριακή φόρτιση (ή όπως αναφέρεται αλλιώς, να μην κατακλύζουν τα υποκείμενα των δεδομένων με πληροφορίες). Ένας τρόπος για να γίνει αυτό μπορεί να είναι οι διαστρωματωμένες επισημάνσεις, όπου τα υποκείμενα ενημερώνονται βήμα προς βήμα για τα δικαιώματά τους (για παράδειγμα, παρέχοντας τις πληροφορίες κλειδιά σε σύντομο χρονικό διάστημα και τις υπόλοιπες - στο σημείο συλλογής των δεδομένων). Αυτές οι πληροφορίες πρέπει να είναι ξεχωριστές από άλλες πληροφορίες που δεν σχετίζονται με την ιδιωτική ζωή, όπως συμβατικές διατάξεις.

Η απαίτηση η πληροφορία να είναι «κατανοητή» σημαίνει ότι θα πρέπει να γίνεται αντιληπτή από ένα μέσο μέλος του στοχευμένου κοινού, στην παρούσα περίπτωση, από τον μέσο πολίτη της τοπικής κοινότητας. Τα υποκείμενα των δεδομένων πρέπει να είναι σε θέση να καθορίζουν εκ των προτέρων ποια είναι η έκταση και οι συνέπειες της επεξεργασίας. Η ομάδα εργασίας του άρθρου 29 (WP29) συνιστά ότι οι υπεύθυνοι επεξεργασίας δεδομένων διευκρινίζουν με σαφή γλώσσα το ποιες θα είναι οι σημαντικότερες συνέπειες της επεξεργασίας, ιδίως αν αυτές οι συνέπειες μπορεί να έχουν αντίκτυπο στα θεμελιώδη δικαιώματα των υποκειμένων[iii].

Το στοιχείο "εύκολη πρόσβαση" σημαίνει ότι το υποκείμενο των δεδομένων δεν θα πρέπει να υποχρεούται να αναζητήσει τις πληροφορίες. Αντ 'αυτού, θα πρέπει να παρουσιάζονται με προφανή τρόπο, έτσι ώστε το υποκείμενο να έχει πρόσβαση χωρίς προσπάθεια.

2.1.2. "Σαφής και απλή γλώσσα"

Η απαίτηση για σαφή και απλή γλώσσα σημαίνει ότι οι πληροφορίες πρέπει να παρέχονται με όσο το δυνατόν απλούστερο τρόπο, αποφεύγοντας τη σύνθετη γλωσσική διάρθρωση και τις πολύπλοκες φράσεις. Οι πληροφορίες δεν πρέπει να διατυπώνονται

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

με αφηρημένους ή αμφιλεγόμενους όρους ή να αφήνουν περιθώρια για διαφορετικές ερμηνείες[iv]. Οι σκοποί και η νομική βάση για την επεξεργασία δεδομένων προσωπικού χαρακτήρα θα πρέπει να είναι σαφείς. Πρέπει να αποφευχθεί κάθε ασαφής διατύπωση των σκοπών επεξεργασίας όπως "για ανάπτυξη μελλοντικών υπηρεσιών" για " έρευνητικούς σκοπούς". Οι πληροφορίες που παρέχονται σε ένα υποκείμενο δεδομένων δεν πρέπει να περιέχουν υπερβολικά νομική, τεχνική ή εξειδικευμένη γλώσσα ή ορολογία[v].

Οι τοπικές αρχές θα πρέπει επίσης να εξασφαλίζουν ότι το λεξιλόγιο, ο τόνος και το στυλ της γλώσσας που χρησιμοποιείται όταν απευθύνονται σε παιδιά είναι κατάλληλα και αντηχούν σε παιδιά έτσι ώστε εκείνα να αναγνωρίζουν ότι το μήνυμα / πληροφορία απευθύνεται προς αυτά[vi].

2.1.3. Τρόπος παροχής πληροφοριών (άρθρο 12, παρ. 1 & παρ. 5 "δωρεάν").

Οι ελεγκτές δεδομένων δεν μπορούν να χρεώνουν τα υποκείμενα δεδομένων για την παροχή πληροφοριών βάσει των άρθρων 13 και 14 (πληροφορίες που πρέπει να παρέχονται στο υποκείμενο των δεδομένων), ή για ανακοινώσεις και δράσεις που λαμβάνονται βάσει των άρθρων 15 - 22 (δικαιώματα των προσώπων στα οποία αναφέρονται τα δεδομένα) και του άρθρου 34 (ανακοίνωση παραβίασης δεδομένων προσωπικού χαρακτήρα στο υποκείμενο των δεδομένων). Υπάρχει μία εξαίρεση από αυτόν τον κανόνα: στην περίπτωση που τα αιτήματα ενός υποκειμένου δεδομένων είναι προδήλως αβάσιμα ή υπερβολικά, ιδίως λόγω του επαναλαμβανόμενου χαρακτήρα τους. Σε αυτή την περίπτωση, ο υπεύθυνος επεξεργασίας μπορεί να επιβάλει την καταβολή εύλογου τέλους, λαμβάνοντας υπόψη τα διοικητικά έξοδα για την παροχή της ενημέρωσης ή την ανακοίνωση ή την εκτέλεση της ζητούμενης ενέργειας. Είναι σημαντικό οι υπεύθυνοι επεξεργασίας δεδομένων να γνωρίζουν ότι φέρουν το βάρος της απόδειξης του προδήλως αβάσιμου ή υπερβολικού χαρακτήρα του αιτήματος. Επομένως, δεν είναι φρόνιμο οι τοπικές αρχές να χρεώνουν τους πολίτες για την παροχή πληροφοριών στο πλαίσιο του ΓΚΠΔ.

2.2. Πληροφορίες που πρέπει να παρέχονται στα πρόσωπα στα οποία αναφέρονται τα δεδομένα (άρθρο 13 & άρθρο 14)

2.2.1. Ποιες πληροφορίες πρέπει να παρέχονται;

Τα άρθρα 13 και 14 του ΓΚΠΔ ορίζουν ποιες πληροφορίες πρέπει να παρέχονται στο υποκείμενο των δεδομένων. Ο Κανονισμός διαφοροποιείται μεταξύ των περιπτώσεων κατά τις οποίες οι πληροφορίες παρέχονται από το υποκείμενο (άρθρο 13) και των περιπτώσεων που δεν παρέχονται (άρθρο 14). Οι τοπικές αρχές θα πρέπει να παρέχουν:

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

1) πληροφορίες σχετικά με την ταυτότητά τους, συμπεριλαμβανομένων των στοιχείων επικοινωνίας τους,
2) Στοιχεία επικοινωνίας του υπεύθυνου προστασίας δεδομένων.
3) τους σκοπούς της επεξεργασίας και της θεμελίωσής τους στο δίκαιο- κυρίως για τις τοπικές αρχές σύμφωνα με το άρθρο 6, παράγραφος 1, στοιχείο ε), η θεμελίωση θα είναι η άσκηση δημόσιας εξουσίας που έχει ανατεθεί στον υπεύθυνο επεξεργασίας, και οι αντίστοιχες διατάξεις της νομοθεσίας του κράτους μέλους ·
4) τον τύπο δεδομένων που βρίσκεται υπό επεξεργασία, όταν δεν έχει δοθεί από το υποκείμενο των δεδομένων
5) την ταυτότητα των πιθανών αποδεκτών των δεδομένων- αυτό δεν περιλαμβάνει μόνο τρίτους, αλλά και επεξεργαστές και από κοινού ελεγκτές. Ο ελεγκτής πρέπει να είναι όσο το δυνατόν πιο συγκεκριμένος κατά τον ορισμό των διαφορετικών κατηγοριών των αποδεκτών δεδομένων.

2.2.2 Ποιες πρόσθετες πληροφορίες πρέπει να παρέχονται;

Πρώτον, για να διασφαλιστεί η δίκαιη και διαφανής επεξεργασία, ο ελεγκτής πρέπει να παράσχει στο υποκείμενο των δεδομένων:

1) το χρονικό διάστημα για το οποίο θα αποθηκευτούν τα δεδομένα προσωπικού χαρακτήρα ή, όταν αυτό είναι αδύνατο, τα κριτήρια που καθορίζουν το εν λόγω διάστημα,
2) την ύπαρξη δικαιώματος υποβολής αιτήματος στον υπεύθυνο επεξεργασίας για πρόσβαση και διόρθωση ή διαγραφή των δεδομένων προσωπικού χαρακτήρα ή περιορισμό της επεξεργασίας που αφορούν το υποκείμενο των δεδομένων ή δικαιώματος αντίταξης στην επεξεργασία, καθώς και δικαιώματος στη φορητότητα των δεδομένων,
3) όταν η επεξεργασία βασίζεται στο άρθρο 6 παράγραφος 1 στοιχείο α) ή στο άρθρο 9 παράγραφος 2 στοιχείο α), την ύπαρξη του δικαιώματος να ανακαλέσει τη συγκατάθεσή του οποτεδήποτε, χωρίς να θιγεί η νομιμότητα της επεξεργασίας που βασίστηκε στη συγκατάθεση πριν από την ανάκλησή της,
4) το δικαίωμα υποβολής καταγγελίας σε εποπτική αρχή,
5) την ύπαρξη αυτοματοποιημένης λήψης αποφάσεων, συμπεριλαμβανομένης της κατάρτισης προφίλ, που αναφέρεται στο άρθρο 22 παράγραφοι 1 και 4 και, τουλάχιστον στις περιπτώσεις αυτές, σημαντικές πληροφορίες σχετικά με τη λογική που ακολουθείται, καθώς και τη σημασία και τις προβλεπόμενες συνέπειες της εν λόγω επεξεργασίας για το υποκείμενο των δεδομένων.

Οι πληροφορίες σχετικά με τον προσδιορισμό του προφίλ πρέπει όχι μόνο να είναι εύκολα προσπελάσιμες για τα υποκείμενα των δεδομένων, αλλά θα πρέπει και να τους

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

γνωστοποιούνται. Ο ελεγκτής θα πρέπει να βρει απλούς τρόπους να ενημερώσει το υποκείμενο των δεδομένων σχετικά με τη λογική ή τα κριτήρια που χρησιμοποιούνται για την αυτοματοποιημένη λήψη αποφάσεων χωρίς πολύπλοκες εξηγήσεις των αλγορίθμων. Όταν τα δεδομένα δεν συλλέγονται από το υποκείμενο των δεδομένων, ο υπεύθυνος επεξεργασίας δεδομένων πρέπει να παρέχει την πηγή του. Εάν το υποκείμενο των δεδομένων συλλέγει τα δεδομένα, ο υπεύθυνος επεξεργασίας πρέπει να τον ενημερώσει εάν η παροχή δεδομένων προσωπικού χαρακτήρα αποτελεί νομική υποχρέωση.
Δεύτερον, οι ελεγκτές θα πρέπει να ενημερώνουν τα υποκείμενα των δεδομένων εάν σκοπεύουν να επεξεργαστούν τα δεδομένα για οποιονδήποτε άλλο σκοπό, διαφορετικό από αυτόν για τον οποίο συλλέχθηκαν τα δεδομένα. Υποκείμενα δεδομένων πρέπει να παρέχονται πληροφορίες σχετικά με αυτόν τον άλλο σκοπό και με οποιεσδήποτε σχετικές περαιτέρω πληροφορίες, ταυτόσημες με τις πληροφορίες που παρέχονται για τον αρχικό σκοπό (περίοδος επεξεργασίας, νομική βάση για τη μεταποίηση κ.λπ.). Κατά τη λήψη δεδομένων, θα ήταν χρήσιμο να ενημερώνονται τα υποκείμενα των δεδομένων για τυχόν μελλοντική επεξεργασία, εάν είναι πιθανό να διεξαχθεί δεδομένης της δραστηριότητας του υπεύθυνου επεξεργασίας.

2.2.3 Πώς πρέπει να παρέχονται οι πληροφορίες;

Ο προεπιλεγμένος τρόπος παροχής πληροφοριών και ανακοινώσεων με τα πρόσωπα στα οποία αναφέρονται τα δεδομένα είναι γραπτή. Ωστόσο, ο ΓΚΠΔ επιτρέπει επίσης την παροχή πληροφοριών με άλλα μέσα, συμπεριλαμβανομένων των ηλεκτρονικών. Σύμφωνα με το WP29, είναι σημαντικό οι μέθοδοι που επιλέγονται για την παροχή των πληροφοριών να είναι κατάλληλες για τις συγκεκριμένες περιστάσεις[vii]. Οι πληροφορίες μπορούν να παρέχονται προφορικά σε υποκείμενο των δεδομένων κατόπιν αιτήματος, εάν οι πληροφορίες ταυτότητάς τους αποδεικνύονται από άλλα (δηλ. μη-προφορικά) μέσα. Υπάρχει μια εξαίρεση από αυτόν τον κανόνα, όσον αφορά τα στοιχεία που οι υπεύθυνοι επεξεργασίας δεδομένων πρέπει να παρέχουν σύμφωνα με το άρθρο. 13 και 14 - οι πληροφορίες αυτές θα μπορούσαν να αποκαλυφθούν στο άτομο χωρίς έλεγχο ταυτότητας. Η προφορική ενημέρωση δεν σημαίνει αναγκαστικά την κατ' ιδίαν παροχή προφορικών πληροφοριών, αλλά αυτοματοποιημένες προφορικές πληροφορίες. Σύμφωνα με το WP29, ο υπεύθυνος επεξεργασίας δεδομένων πρέπει να επιτρέπει στο υποκείμενο των δεδομένων να ακούσει εκ των προτέρων τα προ-εγγεγραμμένα μηνύματα, ιδίως όταν πρόκειται για άτομα με αναπηρία που έχουν προβλήματα όρασης ή για άλλα υποκείμενα δεδομένων τα οποία ενδέχεται να αντιμετωπίζουν δυσκολίες στην πρόσβαση ή την κατανόηση πληροφοριών σε γραπτή μορφή. Επίσης, σε περιπτώσεις προφορικής παροχής πληροφοριών, οι υπεύθυνοι επεξεργασίας δεδομένων θα πρέπει να είναι σε θέση να αποδείξουν ότι συμμορφώνονται με τις απαιτήσεις του ΓΚΠΔ. Για να γίνει αυτό, θα πρέπει να εξασφαλίσουν ότι έχουν αρχείο 1) της αίτησης για πληροφορίες

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

με προφορικά μέσα, 2) τη μέθοδο επαλήθευσης της ταυτότητας του προσώπου στο οποίο αναφέρονται τα δεδομένα και 3) το γεγονός ότι δόθηκαν πληροφορίες στο υποκείμενο των δεδομένων[viii].

2.2.4. Πότε πρέπει να παρέχονται οι πληροφορίες;

Οι πληροφορίες σχετικά με την επεξεργασία δεδομένων προσωπικού χαρακτήρα πρέπει να παρέχονται στο υποκείμενο των δεδομένων κατά τη στιγμή της συλλογής τους (άρθρο 13, παρ. 1). Όταν τα δεδομένα δεν συλλέγονται απευθείας από το υποκείμενο των δεδομένων αλλά από άλλη πηγή, τότε οι πληροφορίες θα πρέπει να παρέχονται στο υποκείμενο των δεδομένων εντός μιας εύλογης προθεσμίας, αλλά το αργότερο εντός ενός μήνα από την παραλαβή, αναλόγως των περιστάσεων της υπόθεσης. Υπάρχουν δύο συγκεκριμένες περιπτώσεις: πρώτον, όταν τα δεδομένα χρησιμοποιούνται για επικοινωνία με το υποκείμενο, οι πληροφορίες πρέπει να παρέχονται το αργότερο κατά τη στιγμή της πρώτης επικοινωνίας με το εν λόγω υποκείμενο · και δεύτερον, αν αναμένεται ότι τα δεδομένα θα γνωστοποιηθούν σε άλλον παραλήπτη, το αργότερο κατά την πρώτη γνωστοποίηση στον αποδέκτη.

Η περίοδος αυτή μπορεί να παραταθεί έως το πολύ τρεις μήνες λόγω της πολυπλοκότητας και του αριθμού των αιτημάτων (για παράδειγμα εάν το αίτημα αφορά πολλαπλές βάσεις δεδομένων).

Ο υπεύθυνος επεξεργασίας πρέπει να ενημερώσει το υποκείμενο των δεδομένων για οποιαδήποτε τέτοια παράταση εντός ενός μηνός από την παραλαβή της αίτησης, μαζί με τους λόγους για την καθυστέρηση και την ενημέρωση σχετικά με τα δικαιώματα του υποκειμένου να υποβάλει καταγγελία.

2.2.5. Πότε πρέπει να παρέχετε ειδοποίηση σε περίπτωση αλλαγών στις πληροφορίες διαφάνειας που πρέπει να παρέχουν οι ελεγκτές δεδομένων;

Σε περιπτώσεις όπου η αλλαγή των πληροφοριών μπορεί να έχει σοβαρές επιπτώσεις στο υποκείμενο των δεδομένων, οι υπεύθυνοι επεξεργασίας δεδομένων πρέπει να παρέχουν πληροφορίες αρκετά πριν από την πραγματική εφαρμογή της αλλαγής[ix]. Οι πολίτες θα πρέπει να έχουν αρκετό χρόνο για να εξετάσουν τη φύση και τον αντίκτυπο της αλλαγής και να ασκήσουν τα δικαιώματά τους βάσει του ΓΚΠΔ σε σχέση με την αλλαγή, για παράδειγμα, να αντιταχθούν στην επεξεργασία. Το WP29 συνιστά την τακτική υπενθύμιση στα υποκείμενα των δεδομένων της εμβέλειας της επεξεργασίας δεδομένων[x].

Όταν σχεδιάζεται η επεξεργασία των δεδομένων για διαφορετικό σκοπό από εκείνον για τον οποίο ελήφθησαν, τα υποκείμενα των δεδομένων θα πρέπει να ενημερώνονται πριν ξεκινήσει η νέα επεξεργασία.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

2.3. Τρόποι

Οι τρόποι είναι οι μορφές στις οποίες οι υπεύθυνοι επεξεργασίας δεδομένων εκπληρώνουν την υποχρέωσή τους βάσει του ΓΚΠΔ να παρέχουν πληροφορίες στα υποκείμενα των δεδομένων.

2.3.1. Σημειώσεις προστασίας προσωπικών δεδομένων/δηλώσεις

Σχετικά με τις διαδικτυακές πλατφόρμες, η χρήση μιας προσέγγισης των δηλωμένων δηλώσεων προστασίας προσωπικών δεδομένων / προειδοποιήσεων για τη σύνδεση με τις διάφορες κατηγορίες πληροφοριών που πρέπει να παρέχονται στο υποκείμενο των δεδομένων, αντί να χρησιμοποιεί μία μόνο ειδοποίηση[xi]. Αυτή η προσέγγιση επιτρέπει στους χρήστες να κατευθύνονται απευθείας στο τμήμα της ειδοποίησης που επιθυμούν να διαβάσουν. Κατά την κατασκευή μιας τέτοιας πολυεπίπεδης ειδοποίησης, οι ελεγκτές πρέπει να επιδιώκουν να παρέχουν μια σαφή και κατανοητή επισκόπηση (ή περιεχόμενο), έτσι ώστε τα υποκείμενα των δεδομένων να γνωρίζουν πού μπορούν να βρουν κάθε πληροφορία.

2.3.2. Σημειώσεις "Push" & "pull"

Η ομάδα εργασίας του άρθρου 29 εισάγει επίσης τη χρήση σημείων "push" και "pull". Η κύρια διαφορά είναι ότι στην τελευταία περίπτωση οι χρήστες ενός ιστότοπου προβλέπεται να μπορούν να ζητήσουν πληροφορίες, στην συγκεκριμένη περίπτωση πληροφορίες σχετικά με την επεξεργασία των δεδομένων τους, ενώ στην προηγούμενη περίπτωση, η ειδοποίηση "ωθείται" στην οθόνη τους χωρίς καμία ενέργεια από την πλευρά τους. Το WP29 παρέχει παραδείγματα και ορισμούς για ειδοποιήσεις push με ειδοποιήσεις πληροφοριών διαφάνειας "just-in-time" και για ειδοποιήσεις "pull" - με πίνακες ελέγχου διαφάνειας και "μάθετε περισσότερα" μαθήματα[xii]:

- Μια ειδοποίηση just-in-time χρησιμοποιείται για να παρέχει συγκεκριμένες «ιδιωτικές πληροφορίες» όταν αυτό είναι το πλέον σημαντικό για να διαβάσει το υποκείμενο των δεδομένων. Αυτή η μορφή μπορεί να είναι χρήσιμη όταν ένας ιστότοπος μιας τοπικής αρχής προβλέπει την εκτέλεση μιας συγκεκριμένης υπηρεσίας στο διαδίκτυο μετά την συμπλήρωση μιας φόρμας. Πριν ο πολίτης καταθέσει τη φόρμα, μια τέτοια just-in-time ειδοποίηση μπορεί να εμφανιστεί.
- Ο πίνακας ελέγχου διαφάνειας είναι ένα μόνο σημείο από το οποίο τα άτομα μπορούν να δουν τις ιδιωτικές και να διαχειριστούν τις προτιμήσεις τους για την προστασία της ιδιωτικής ζωής, είτε επιτρέποντας ή παρεμποδίζοντας τη χρήση των δεδομένων τους με ορισμένους τρόπους.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

2.3.3. Άλλοι τύποι "κατάλληλων μέτρων"

Εκτός από το ψηφιακό περιβάλλον, σύμφωνα με το WP29 κατάλληλο μέτρο θα μπορούσε να είναι:

- Για έντυπο / χάρτινο περιβάλλον: γραπτές εξηγήσεις, φυλλάδια.
- Τηλεφωνικό περιβάλλον: προφορικές εξηγήσεις από πραγματικό πρόσωπο, αυτοματοποιημένες ή προ-καταγεγγραμμένες πληροφορίες με επιλογές ακρόασης λεπτομερέστερων πληροφοριών.
- Κωδικοί γρήγορης ανταπόκρισης, ειδοποιήσεις φωνής, γραπτές πληροφορίες σχετικά με την έξυπνη συσκευή, μηνύματα που αποστέλλονται με SMS ή ηλεκτρονικό ταχυδρομείο και άλλα.
- Δια ζώσης περιβάλλον: προφορικές εξηγήσεις, γραπτές εξηγήσεις που παρέχονται σε μορφή σκληρού ή μαλακού αντιγράφου[xiii].

2.3.4. Οπτικοποίηση

Ο ΓΚΠΔ εισάγει εργαλεία οπτικοποίησης (κυρίως αναφορικά, με εικόνες, μηχανισμούς πιστοποίησης, και σφραγίδες και σήματα προστασίας δεδομένων). Η ιδέα των εικονιδίων είναι να μεταδώσουν τις πληροφορίες στα υποκείμενα των δεδομένων με προσπελάσιμο τρόπο, χρησιμοποιώντας τυποποιημένα σύμβολα / εικόνες, αναγνωρίσιμα σε ολόκληρη την ΕΕ. Η ανάπτυξη ενός "κώδικα των εικονιδίων" δεν έχει ξεκινήσει ακόμα. Ο ΓΚΠΔ προβλέπει επίσης τη χρήση μηχανισμών πιστοποίησης προστασίας δεδομένων, σφραγίδων και σημάτων προστασίας δεδομένων με σκοπό την απόδειξη της συμμόρφωσης με τον κανονισμό. Οι μηχανισμοί πιστοποίησης θεσπίζονται από τα κράτη μέλη, τις εποπτικές αρχές, τον Ευρωπαϊκό Οργανισμό για την προστασία των δεδομένων ή την Επιτροπή και προορίζονται να αποδείξουν ότι ο ελεγκτής συμμορφώνεται με τον ΓΕΚΠΔ, αποδεικνύοντας ότι εφαρμόζει τεχνικά και οργανωτικά μέτρα για την εκπλήρωση των προτύπων για την προστασία των δεδομένων. Αυτές οι μορφές μπορούν να εφαρμοστούν σε οντότητες που δεν είναι δημόσιες αρχές, όπως σε μια αυτόνομη δημοτική επιχείρηση.

2.4. Άσκηση των δικαιωμάτων των υποκειμένων των δεδομένων

Τα υποκείμενα δεδομένων έχουν το δικαίωμα να λαμβάνουν πληροφορίες από τους υπεύθυνους επεξεργασίας δεδομένων σχετικά με τα προσωπικά τους δεδομένα. Οι πληροφορίες που πρέπει να παρέχονται στο πλαίσιο του ΓΚΠΔ αναφέρονται ρητά στο άρθρο 13 και στο άρθρο 14 και τα υποκείμενα των δεδομένων δεν χρειάζεται να υποβάλλουν αίτημα ή να λάβουν άλλα ενεργά μέτρα για να τις αποκτήσουν, σε αντίθεση με την διαδικασία άσκησης των άλλων δικαιωμάτων τους (δικαίωμα πρόσβασης, διόρθωσης, διαγραφής κ.λπ.).

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

2.4.1. Εξαιρέσεις από την υποχρέωση παροχής πληροφοριών

Το δικαίωμα στην πληροφόρηση δεν είναι απόλυτο, ή με άλλα λόγια, είναι περιορισμένο σε ορισμένες περιπτώσεις.

Σε ορισμένες περιπτώσεις, οι τοπικές αρχές εξαιρούνται από την υποχρέωση παροχής των προαναφερθεισών πληροφοριών που περιγράφονται στο άρθρο. 13 & 14. Όταν τα δεδομένα συλλέγονται από το υποκείμενο των δεδομένων, μια τέτοια περίπτωσηθα μπορούσε να είναι όταν αυτός/αυτή έχει ήδη συλλέξει τις πληροφορίες (άρθρο 13, παρ. 4).

Όταν τα δεδομένα δεν συλλέγονται από το υποκείμενο, οι εξαιρέσεις είναι περισσότερες (άρθρο 14, παράγραφος 5):

- όταν το υποκείμενο των δεδομένων έχει ήδη τις πληροφορίες.
- όταν η παροχή τέτοιων πληροφοριών αποδεικνύεται αδύνατη, ή θα συνεπαγόταν δυσανάλογη προσπάθεια ή θα καθιστούσε αδύνατη την επίτευξη των στόχων της επεξεργασίας ή θα μπορούσε να την βλάψει σοβαρά. Ένα παράδειγμα αδυναμίας παροχής πληροφοριών είναι όταν ο υπεύθυνος της επεξεργασίας δεν έχει κανένα μέσο επικοινωνίας με το υποκείμενο των δεδομένων.
- όταν η απόκτηση ή η δημοσιοποίηση ορίζεται ρητά από το δίκαιο των κρατών μελών της ΕΕ ή την ΕΕ, η οποία θα ήταν η συνηθέστερη υπόθεση για τις τοπικές αρχές.
- όταν τα προσωπικά δεδομένα υπόκεινται σε υποχρέωση επαγγελματικού απορρήτου που διέπεται από το δίκαιο της Ένωσης ή του κράτους μέλους, συμπεριλαμβανομένης της υποχρεωτικής φύλαξης του απορρήτου · αυτή η εξαίρεση μπορεί να ισχύει για αυτόνομες δημοτικές επιχειρήσεις και παρόμοιες οντότητες.

Σύμφωνα με το WP29[xiv], οι εξαιρέσεις αυτές πρέπει, κατά γενικό κανόνα, να ερμηνεύονται και να εφαρμόζονται στενά.

3. ΣΥΜΠΕΡΑΣΜΑ ΚΑΙ ΠΡΑΚΤΙΚΕΣ ΣΥΜΒΟΥΛΕΣ

Η αρχή της διαφάνειας είναι ένα από τα θεμέλια του ΓΚΠΔ. Διασφαλίζει με πολλούς τρόπους ότι τα φυσικά πρόσωπα έχουν όλες τις πληροφορίες που χρειάζονται προκειμένου αρχικά να ενημερωθούν για τα δεδομένα προσωπικού χαρακτήρα που βρίσκονται σε επεξεργασία και τους αφορούν και έπειτα να ασκήσουν τα δικαιώματά τους βάσει του κανονισμού. Οι πληροφορίες πρέπει να είναι εύκολα προσβάσιμες και κατανοητές με σαφή και απλή γλώσσα.

Συνιστάται στις τοπικές αρχές να καταρτίσουν μια λίστα με όλες τις πληροφορίες που απαιτούνται από τον ΓΚΠΔ και να επιλέξουν τις καλύτερες μεθόδους για να προσεγγίσουν

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

τους πολίτες, των οποίων τα δεδομένα επεξεργάζονται. Για παράδειγμα, μπορούν να βάζουν ενημερωτικά δελτία πληροφοριών στα δημόσια γραφεία και να παρέχουν φυλλάδια που περιλαμβάνουν τις πληροφορίες που αναφέρονται στο άρθρο 13 και το άρθρο 14 και να τα διανέμουν. Τα ηλεκτρονικά μέσα μπορεί να είναι χρήσιμα, για παράδειγμα εάν η οντότητα διαθέτει έναν διαδικτυακό ιστότοπο / πλατφόρμα, αλλά σε ορισμένες περιπτώσεις μπορεί να είναι απαραίτητη και η έντυπη μορφή. Ιδιαίτερη προσοχή πρέπει να δοθεί όταν οι δικτυακές πύλες των τοπικών αρχών προσφέρουν ηλεκτρονικές υπηρεσίες. Επίσης, θα πρέπει να ληφθεί υπόψη ότι ορισμένες αυτόνομες δημοτικές επιχειρήσεις (όπως οι εταιρείες δημοσίων μεταφορών, για παράδειγμα) εκτελούν πολυάριθμες επεξεργασίες και ασχολούνται με τεράστιες βάσεις δεδομένων και, ως εκ τούτου, πρέπει να καταβάλουν επιπλέον προσπάθειες για τη σωστή σύνταξη των πληροφοριών στο πλαίσιο του άρθρου 13 και 14.

LATVIAN ASSOCIATION OF LOCAL AND REGIONAL GOVERNMENTS

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

4. ΕΞΩΤΕΡΙΚΕΣ ΠΗΓΕΣ & ΔΙΑΔΙΚΤΥΑΚΟΙ ΣΥΝΔΕΣΜΟΙ

Βιβλία

- **Voigt, P., von dem Bussche, A.**, The EU General Data Protection Regulation (GDPR) – A Practical Guide, Springer International Publishing (2017);
- Bird & Bird Guide to General Data Protection Regulation (2016);
- EU General Data Protection Regulation (GDPR). An Implementation and Compliance Guide, IT Governance Publishing, Cambridgeshire (2016);

Έγγραφα της ομάδας εργασίας του άρθρου 29

- Article 29 Data Protection Working Party, Guidelines on transparency under Regulation 2016/679, WP260;

Διαδικτυακοί σύνδεσμοι

- http://europa.eu/rapid/press-release_IP-18-386_en.htm
- https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en

5. ΠΑΡΑΠΟΜΠΕΣ

[i] The Article 29 Working Party (WP) is established on the basis of Art. 29 of Directive 95/46/EC, which will be replaced by the GDPR. The goal of the WP is to provide opinions and recommendations and to advice on personal data protection.
[ii] Article 29 Data Protection Working Party, Guidelines on transparency under Regulation 2016/679, p. 23
[iii] Ibid, p. 8
[iv] Ibid, p. 9
[v] Ibid
[vi] Ibid
[vii] Ibid, p. 21
[viii] Ibid, p. 12
[ix] Ibid, p. 15
[x] Ibid, p. 16
[xi] Ibid, p. 17
[xii] Ibid, p. 17-18
[xiii] Ibid, p. 18-19
[xiv] Ibid, p. 25

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

ProLegis

Κοινοποίηση πληροφοριών ή Δικαίωμα πρόσβασης από το υποκείμενο των δεδομένων

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

Contents

1. Νομικό πλαίσιο 3

1.1. ΓΚΠΔ 3

2. Βασικά 5

3. Λεπτομέρειες σχετικά με την κοινοποίηση πληροφοριών στο υποκείμενο των δεδομένων 6

3.1. Περιεχόμενο της κοινοποίησης 6

3.2. Πόση ώρα έχει ο υπεύθυνος επεξεργασίας για να απαντήσει; (χρονικό περιθώριο); 7

3.3. Με ποια μορφή μπορεί να αξιωθεί και πώς πρέπει να απαντηθεί; 7

3.4. Πρέπει να αποδειχθεί η ταυτότητα του αιτούντος ως υποκειμένου των δεδομένων; 8

3.5. Έξοδα; Είναι δυνατόν να επιστραφούν οι πληροφορίες; 9

3.6. Υπάρχει υποχρέωση του αιτούντος να συμμετάσχει στην πληροφόρηση; 9

3.7. Τα δικαιώματα τρίτων πρέπει να λαμβάνονται υπόψη κατά την παροχή πληροφοριών; 9

4. Λίστα ελέγχου για την παροχή πληροφοριών κατόπιν αιτήσεως 11

4.1. Έκδοση των πληροφοριών 12

5. Εξωτερικές πηγές & Διαδικτυακοί Σύνδεσμοι 14

5.1. Βιβλία και άρθρα 14

5.2. Άλλα έγγραφα και υποθέσεις 14

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

1. Νομικό πλαίσιο

1.1. ΓΚΠΔ

Άρθρο 15

Δικαίωμα πρόσβασης του υποκειμένου των δεδομένων

1. Το υποκείμενο των δεδομένων έχει το δικαίωμα να λαμβάνει από τον υπεύθυνο επεξεργασίας επιβεβαίωση για το κατά πόσον ή όχι τα δεδομένα προσωπικού χαρακτήρα που το αφορούν υφίστανται επεξεργασία και, εάν συμβαίνει τούτο, το δικαίωμα πρόσβασης στα δεδομένα προσωπικού χαρακτήρα και στις ακόλουθες πληροφορίες:

(α) τους σκοπούς της επεξεργασίας,

(β) τις σχετικές κατηγορίες δεδομένων προσωπικού χαρακτήρα,

(γ) τους αποδέκτες ή τις κατηγορίες αποδεκτών στους οποίους κοινολογήθηκαν ή πρόκειται να κοινολογηθούν τα δεδομένα προσωπικού χαρακτήρα, ιδίως τους αποδέκτες σε τρίτες χώρες ή διεθνείς οργανισμούς,

(δ) εάν είναι δυνατόν, το χρονικό διάστημα για το οποίο θα αποθηκευτούν τα δεδομένα προσωπικού χαρακτήρα ή, όταν αυτό είναι αδύνατο, τα κριτήρια που καθορίζουν το εν λόγω διάστημα,

(ε) την ύπαρξη δικαιώματος υποβολής αιτήματος στον υπεύθυνο επεξεργασίας για διόρθωση ή διαγραφή δεδομένων προσωπικού χαρακτήρα ή περιορισμό της επεξεργασίας των δεδομένων προσωπικού χαρακτήρα που αφορά το υποκείμενο των δεδομένων ή δικαιώματος αντίταξης στην εν λόγω επεξεργασία,

(στ) το δικαίωμα υποβολής καταγγελίας σε εποπτική αρχή,

(ζ) όταν τα δεδομένα προσωπικού χαρακτήρα δεν συλλέγονται από το υποκείμενο των δεδομένων, κάθε διαθέσιμη πληροφορία σχετικά με την προέλευσή τους,

(η) την ύπαρξη αυτοματοποιημένης λήψης αποφάσεων, συμπεριλαμβανομένης της κατάρτισης προφίλ, που προβλέπεται στο άρθρο 22 παράγραφοι 1 και 4 και, τουλάχιστον στις περιπτώσεις αυτές, σημαντικές πληροφορίες σχετικά με τη λογική που ακολουθείται, καθώς και τη σημασία και τις προβλεπόμενες συνέπειες της εν λόγω επεξεργασίας για το υποκείμενο των δεδομένων.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

2. Όταν δεδομένα προσωπικού χαρακτήρα διαβιβάζονται σε τρίτη χώρα ή σε διεθνή οργανισμό, το υποκείμενο των δεδομένων έχει το δικαίωμα να ενημερώνεται για τις κατάλληλες εγγυήσεις σύμφωνα με το άρθρο 46 σχετικά με τη διαβίβαση.

3. Ο υπεύθυνος επεξεργασίας παρέχει αντίγραφο των δεδομένων προσωπικού χαρακτήρα που υποβάλλονται σε επεξεργασία. Για επιπλέον αντίγραφα που ενδέχεται να ζητηθούν από το υποκείμενο των δεδομένων, ο υπεύθυνος επεξεργασίας μπορεί να επιβάλει την καταβολή εύλογου τέλους για διοικητικά έξοδα. Εάν το υποκείμενο των δεδομένων υποβάλλει το αίτημα με ηλεκτρονικά μέσα και εκτός εάν το υποκείμενο των δεδομένων ζητήσει κάτι διαφορετικό, η ενημέρωση παρέχεται σε ηλεκτρονική μορφή που χρησιμοποιείται συνήθως.

4. Το δικαίωμα να λαμβάνεται αντίγραφο που αναφέρεται στην παράγραφο 3 δεν επηρεάζει δυσμενώς τα δικαιώματα και τις ελευθερίες άλλων.

Recitals 63 and 64:

(63) Ένα υποκείμενο των δεδομένων θα πρέπει να έχει δικαίωμα πρόσβασης σε δεδομένα προσωπικού χαρακτήρα τα οποία συλλέχθηκαν και το αφορούν και να μπορεί να ασκεί το εν λόγω δικαίωμα ευχερώς και σε εύλογα τακτά διαστήματα, προκειμένου να έχει επίγνωση και να επαληθεύει τη νομιμότητα της επεξεργασίας. Αυτό περιλαμβάνει το δικαίωμα των υποκειμένων των δεδομένων να έχουν πρόσβαση στα δεδομένα που αφορούν την υγεία τους, για παράδειγμα τα δεδομένα των ιατρικών αρχείων τους τα οποία περιέχουν πληροφορίες όπως διαγνώσεις, αποτελέσματα εξετάσεων, αξιολογήσεις από θεράποντες ιατρούς και κάθε παρασχεθείσα θεραπεία ή επέμβαση. Επομένως, κάθε υποκείμενο των δεδομένων θα πρέπει να έχει το δικαίωμα να γνωρίζει και να του ανακοινώνεται ιδίως για ποιους σκοπούς γίνεται η επεξεργασία των δεδομένων προσωπικού χαρακτήρα, εφόσον είναι δυνατόν για πόσο διάστημα γίνεται η επεξεργασία των δεδομένων προσωπικού χαρακτήρα, ποιοι αποδέκτες λαμβάνουν τα δεδομένα προσωπικού χαρακτήρα, ποια λογική ακολουθείται στην τυχόν αυτόματη επεξεργασία δεδομένων προσωπικού χαρακτήρα και ποιες θα μπορούσαν να είναι οι συνέπειες της εν λόγω επεξεργασίας, τουλάχιστον όταν αυτή βασίζεται σε κατάρτιση προφίλ. Ο υπεύθυνος επεξεργασίας θα πρέπει να δύναται να παρέχει πρόσβαση εξ αποστάσεως σε ασφαλές σύστημα μέσω του οποίου το υποκείμενο των δεδομένων αποκτά άμεση πρόσβαση στα δεδομένα που το αφορούν. Το δικαίωμα αυτό δεν θα πρέπει να επηρεάζει αρνητικά τα δικαιώματα ή τις ελευθερίες άλλων, όπως το επαγγελματικό απόρρητο ή το δικαίωμα διανοητικής ιδιοκτησίας και, ειδικότερα, το δικαίωμα δημιουργού που προστατεύει το λογισμικό. Ωστόσο, οι παράγοντες αυτοί δεν θα πρέπει να έχουν ως αποτέλεσμα την άρνηση παροχής κάθε πληροφορίας στο υποκείμενο των δεδομένων. Όταν ο υπεύθυνος επεξεργασίας επεξεργάζεται μεγάλες ποσότητες πληροφοριών σχετικά με το υποκείμενο

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

των δεδομένων, ο υπεύθυνος επεξεργασίας θα πρέπει να δύναται να ζητεί από το υποκείμενο, πριν δοθούν οι πληροφορίες, να προσδιορίζει τις πληροφορίες ή τις δραστηριότητες επεξεργασίας που σχετίζονται με το αίτημα.

(64) Ο υπεύθυνος επεξεργασίας θα πρέπει να χρησιμοποιεί κάθε εύλογο μέτρο για να επαληθεύει την ταυτότητα του υποκειμένου των δεδομένων το οποίο ζητεί πρόσβαση, ιδίως στο πλαίσιο επιγραμμικών υπηρεσιών και επιγραμμικών αναγνωριστικών στοιχείων ταυτότητας. Ο υπεύθυνος επεξεργασίας δεν θα πρέπει να διατηρεί δεδομένα προσωπικού χαρακτήρα με μοναδικό σκοπό να μπορεί να αποκρίνεται σε δυνητικά αιτήματα.

2. Βασικά

Ο ΓΚΠΔ προβλέπει στο άρθρο 15 το δικαίωμα κοινοποίησης όλων των διαθέσιμων πληροφοριών στο υποκείμενο των δεδομένων κατόπιν αιτήσεώς του (π.χ. πελάτης, υπάλληλος, αιτών εργασία, ασθενής, εφεξής καλούμενο "υποκείμενο των δεδομένων") έναντι του υπευθύνου της επεξεργασίας (π.χ. εταιρεία, εργοδότης, διαχειριστής νοσοκομείων). Αυτό καλείται "Δικαίωμα πρόσβασης του υποκειμένου των δεδομένων (στα δεδομένα της / του). Ο σκοπός αυτού του δικαιώματος αφορά στο ότι το υποκείμενο των δεδομένων μπορεί να λάβει πληροφορίες ως προς το περιεχόμενο και τις λεπτομέρειες των δεδομένων που υφίστανται επεξεργασία σχετικά με αυτόν / αυτήν, με σκοπό την ενδεχόμενη εξασφάλιση περαιτέρω δικαιωμάτων του υποκειμένου των δεδομένων (π.χ. διόρθωση ή διαγραφή σύμφωνα με το άρθρο 16 του ΓΚΠΔ) ή τη νομιμότητα της επεξεργασίας.

Το δικαίωμα αυτό αποτελεί κεντρικό θεσμικό όργανο της νομοθεσίας για την προστασία των δεδομένων, καθώς συχνά πρέπει να θεωρείται ως βάση προκειμένου το υποκείμενο των δεδομένων να ασκεί οποιαδήποτε άλλα δικαιώματα. Παρότι οι Αρχές Προστασίας Δεδομένων (DPAs) στο πλαίσιο του ΓΚΠΔ έχουν την εξουσία να ελέγχουν έναν υπεύθυνο επεξεργασίας χωρίς συγκεκριμένη καταγγελία, στην πράξη (λόγω περιορισμένων πόρων των ΑΠΔ) αυτή είναι συνήθως μια ελλιπής ή καθυστερημένη κοινοποίηση σύμφωνα με το δικαίωμα πρόσβασης των υποκειμένων το οποίο ζητεί τις ΑΠΔ σχετικά με το σχέδιο. Έτσι, οι υπεύθυνοι επεξεργασίας οφείλουν να είναι καλά προετοιμασμένοι για αυτή τη διαδικασία.

Η καλύτερη προετοιμασία ωστόσο είναι τα ορθώς δομημένα και κατά το δυνατόν λεπτομερέστερα αρχεία των δραστηριοτήτων επεξεργασίας. Όσο καλύτερα διαμορφώνεται αυτή η τεκμηρίωση κατά τις επιχειρηματικές διαδικασίες για τις οποίες γίνεται η επεξεργασία δεδομένων προσωπικού χαρακτήρα, τόσο ευκολότερη είναι η εύρεση των συγκεκριμένων δεδομένων ενός συγκεκριμένου υποκειμένου εντός των αιτήσεων και σε εύθετο χρόνο.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

3. Λεπτομέρειες σχετικά με την κοινοποίηση πληροφοριών στο υποκείμενο των δεδομένων

3.1. Περιεχόμενο της κοινοποίησης

Το δικαίωμα πρόσβασης παρέχει στο υποκείμενο των δεδομένων τα εξής:

i. Το δικαίωμα να ζητήσει από τον υπεύθυνο της επεξεργασίας να επιβεβαιώσει εάν το προσωπικό του / της είναι υπό επεξεργασία ή όχι ˙ εάν είναι απαραίτητο, μια ερώτηση θα πρέπει επίσης να απαντηθεί «αρνητικά» εφόσον δεδομένα σχετικά με αυτό το άτομο δεν έχουν υποστεί επεξεργασία (αποκαλούμενες "αρνητικές πληροφορίες"): "Δεν επεξεργαζόμαστε δεδομένα σχετικά με εσάς".;

ii. Το δικαίωμα λήψης αντιγράφου των δεδομένων προσωπικού χαρακτήρα που αποτελούν αντικείμενο της επεξεργασίας (για τυχόν επιπλέον αντίγραφα που ζητούνται από το υποκείμενο των δεδομένων, ο υπεύθυνος επεξεργασίας μπορεί να χρεώσει εύλογη αμοιβή με βάση τα διοικητικά έξοδα. Εάν το υποκείμενο των δεδομένων καταθέσει ηλεκτρονικά την αίτηση, τότε οι πληροφορίες παρέχονται σε κοινή ηλεκτρονική μορφή, εκτός αν ορίζεται διαφορετικά.

iii. Το δικαίωμα απόκτησης των ακολούθων πληροφοριών:

Άρθρο 15 παρ. 1 ΓΚΠΔ	**Περιεχόμενο των πληροφοριών**
Σημείο α	ο σκοπός της επεξεργασίας
Σημείο β	οι κατηγορίες επεξεργασμένων προσωπικών δεδομένων
Σημείο γ	οι παραλήπτες ή οι κατηγορίες παραληπτών στους οποίους έχουν διαβιβαστεί ή θα μπορούσαν να γνωστοποιηθούν τα προσωπικά δεδομένα, ιδίως οι αποδέκτες σε τρίτες χώρες ή διεθνείς οργανισμούς
Σημείο δ	όπου είναι δυνατόν, η προβλεπόμενη περίοδος κατά την οποία αποθηκεύονται τα προσωπικά δεδομένα ή, εάν δεν είναι δυνατόν, τα κριτήρια που χρησιμοποιούνται για τον καθορισμό της εν λόγω περιόδου;
Σημείο ε	η ύπαρξη του δικαιώματος αίτησης από τον υπεύθυνο της επεξεργασίας για διόρθωση ή διαγραφή δεδομένων προσωπικού χαρακτήρα ή περιορισμό της επεξεργασίας δεδομένων προσωπικού χαρακτήρα σχετικά με το πρόσωπο στο οποίο αναφέρονται τα δεδομένα ή αντίταξης στην εν λόγω επεξεργασία;
Σημείο στ	το δικαίωμα υποβολής καταγγελίας σε εποπτική αρχή;
Σημείο ζ	όταν τα δεδομένα προσωπικού χαρακτήρα δεν συλλέγονται από το υποκείμενο των δεδομένων, κάθε διαθέσιμη πληροφορία σχετικά με την πηγή τους;

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

Σημείο η	η ύπαρξη αυτοματοποιημένης λήψης αποφάσεων, συμπεριλαμβανομένης της κατάρτισης προφίλ, που αναφέρεται στο άρθρο 22 παρ. 1 και 4 και, τουλάχιστον στις περιπτώσεις αυτές, σημαντικές πληροφορίες σχετικά με τη σχετική λογική, καθώς και τη σημασία και τις προβλεπόμενες συνέπειες αυτής της επεξεργασίας για το υποκείμενο των δεδομένων.
Παρ. 2	όταν τα δεδομένα προσωπικού χαρακτήρα μεταφέρονται σε τρίτη χώρα ή σε διεθνή οργανισμό, το υποκείμενο των δεδομένων έχει το δικαίωμα να ενημερώνεται για τα κατάλληλα μέτρα προστασίας σύμφωνα με το άρθρο 46 σχετικά με τη μεταφορά.

Σημείωση: Σύμφωνα με το άρθρο 23, το δικαίωμα ενημέρωσης θα μπορούσε να περιοριστεί από την εθνική νομοθεσία.

3.2. Πόση ώρα έχει ο υπεύθυνος επεξεργασίας για να απαντήσει; (χρονικό περιθώριο);

Κατ 'αρχήν, πρέπει να δοθεί άμεση απάντηση στην αίτηση παροχής πληροφοριών, αλλά το αργότερο εντός ενός μηνός από την παραλαβή της αίτησης (Άρθρο 12 (3) ΓΚΠΔ). Η περίοδος αυτή μπορεί να παραταθεί για περαιτέρω δύο μήνες, εφόσον είναι αναγκαίο, λαμβάνοντας υπόψη την πολυπλοκότητα και τον αριθμό των αιτήσεων. Ο υπεύθυνος επεξεργασίας ενημερώνει το υποκείμενο των δεδομένων σχετικά με την παράταση της προθεσμίας εντός ενός μηνός από την παραλαβή της αίτησης, μαζί με τους λόγους της καθυστέρησης. Εάν το ενδιαφερόμενο πρόσωπο υποβάλει την αίτηση ηλεκτρονικά, το υποκείμενο των δεδομένων πρέπει, ει δυνατόν, να ενημερώνεται με ηλεκτρονικά μέσα, εκτός αν ορίζεται διαφορετικά.

Εάν ο υπεύθυνος επεξεργασίας δεν ενεργήσει βάσει του αιτήματος του υποκειμένου των δεδομένων, θα ενημερώσει το υποκείμενο των δεδομένων χωρίς καθυστέρηση, αλλά το αργότερο ένα μήνα μετά την παραλαβή της αίτησης, σχετικά με τους λόγους και τη δυνατότητα υποβολής γραπτής διαμαρτυρίας σε εποπτική αρχή ή να ασκήσει ένδικα μέσα.

3.3. Με ποια μορφή μπορεί να αξιωθεί και πώς πρέπει να απαντηθεί;

Δεν υπάρχει κανένας περιορισμός όσον αφορά στη μορφή · το αίτημα για πληροφόρηση μπορεί να υποβληθεί προφορικώς, γραπτώς ή σε ψηφιακή μορφή (μέσω ηλεκτρονικού ταχυδρομείου για παράδειγμα). Η απάντηση σε μια αίτηση παροχής πληροφοριών μπορεί να υποβληθεί σε οποιαδήποτε κατάλληλη μορφή, αλλά πρέπει να σημειωθούν τα εξής:

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

- Μια γραπτή αίτηση είναι καλύτερο να απαντάται γραπτώς. Μια κοινή μέθοδος στο παρελθόν ήταν να συνυποβάλλει ο αιτών στην αίτησή του αντίγραφο ταυτότητας (επίσημο δελτίο ταυτότητας) και ο υπεύθυνος να δίνει την απάντηση ως συστημένη επιστολή (με εξαίρεση τους πράκτορες παράδοσης). Καθώς ωστόσο το επίσημο δελτίο ταυτότητας περιέχει συνήθως μεγαλύτερο αριθμό δεδομένων από όσα είναι απαραίτητα για την αναγνώριση του υποκειμένου των δεδομένων, συνιστάται να υποβάλλονται γραπτώς από το υποκείμενο των δεδομένων μόνο πληροφορίες σχετικά με το όνομα, ο προσωπικός αριθμός αναγνώρισης και / ή ο αύξων αριθμός του δελτίου ταυτότητας.
- Εάν απαιτείται από τον αιτούντα, οι πληροφορίες μπορούν να παρέχονται προφορικά, υπό την προϋπόθεση ότι η ταυτότητα του υποκειμένου των δεδομένων έχει καθοριστεί με άλλη μορφή.
- Εάν το υποκείμενο των δεδομένων υποβάλλει την αίτηση ηλεκτρονικά (π.χ. μέσω ηλεκτρονικού ταχυδρομείου), οι πληροφορίες παρέχονται σε κοινή ηλεκτρονική μορφή, εκτός αν ορίζεται διαφορετικά. Εάν είναι δυνατόν, ο υπεύθυνος επεξεργασίας μπορεί επίσης να παρέχει απομακρυσμένη πρόσβαση σε ένα ασφαλές σύστημα το οποίο παρέχει στο υποκείμενο των δεδομένων άμεση πρόσβαση στις προσωπικές του πληροφορίες.

Προσοχή! Όλες οι επικοινωνίες πρέπει να μεταφέρονται σε σαφή και απλή γλώσσα με ακριβή, διαφανή, κατανοητή και εύκολα προσβάσιμη μορφή (αυτό αφορά ιδιαιτέρως σε πληροφορίες που απευθύνονται ειδικά σε παιδιά). Όπως και στο παρελθόν, οι συντομογραφίες που περιέχονται στην απάντηση πρέπει να εξηγούνται από τον υπεύθυνο επεξεργασίας στην απάντησή του.

3.4. Πρέπει να αποδειχθεί η ταυτότητα του αιτούντος ως υποκειμένου των δεδομένων;

Ναί. Η ταυτότητα του προσώπου που ζητεί τις πληροφορίες (του ενδιαφερομένου) πρέπει να είναι σαφής, καθώς ο υπεύθυνος της επεξεργασίας μπορεί να ζητήσει συμπληρωματικές πληροφορίες εάν έχει «εύλογη αμφιβολία» σχετικά με την ταυτότητα του φυσικού προσώπου που υποβάλλει την αίτηση (βλ. Άρθρο 12 παράγραφος 6[1]).

Σύμφωνα με την αιτιολογική έκθεση 64, ο υπεύθυνος επεξεργασίας πρέπει να χρησιμοποιήσει όλα τα εύλογα μέσα προκειμένου να επαληθεύσει την ταυτότητα του υποκειμένου των δεδομένων που αναζητεί πληροφορίες, ιδίως στο πλαίσιο των ηλεκτρονικών υπηρεσιών.

Ο έλεγχος ταυτότητας πρέπει να σχεδιαστεί προκειμένου να εκπληρωθεί η υποχρέωση διασφάλισης της προστασίας δεδομένων σε συνάρτηση με τον κίνδυνο, διαφορετικά

[1] See also Souhrada-Kirchmayer, The right of access to the DSGVO, in Jahnel [Hrsg], Yearbook 17. Data Protection Law [2017] 86 f.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

μπορεί να υπάρξει παραβίαση δεδομένων εάν τα δεδομένα μεταδοθούν σε λάθος παραλήπτη.

Μια κοινή πρακτική στην Αυστρία βάσει του προηγουμένου νόμου περί προστασίας δεδομένων (DSG 2000) ήταν να συνυποβάλλει στην αίτησή του αντίγραφο εγγράφου ταυτότητας (επίσημο δελτίο ταυτότητας) και ο υπεύθυνος της επεξεργασίας να δίνει την απάντηση στο ταχυδρομείο ως «προσωπική» συστημένη επιστολή (εκτός εξουσιοδοτημένων αντιπροσώπων). Ωστόσο, η ταυτότητα μπορεί επίσης να είναι ξεκάθαρη από την κατάσταση, π.χ. εάν υπάρχει συνεχής επαφή με τον πάροχο πληροφοριών και αυτή (και η διεύθυνση του)είναι γνωστή[2].

3.5. Έξοδα; Είναι δυνατόν να επιστραφούν οι πληροφορίες;

Κατ 'αρχήν, οι πληροφορίες πρέπει να παρέχονται δωρεάν (βλέπε Άρθρο 12 παράγραφος 5 του ΓΚΠΔ). Ωστόσο, σε περίπτωση προδήλως αβάσιμων ή, ιδίως σε περίπτωση συχνής επανάληψης, υπερβολικών αιτημάτων από υποκείμενο των δεδομένων, ο υπεύθυνος επεξεργασίας μπορεί:

(α) να απαιτήσει εύλογη αμοιβή, λαμβάνοντας υπόψη τις διοικητικές δαπάνες για την ενημέρωση ή την επικοινωνία ή την εφαρμογή του ζητούμενου μέτρου · ή

(β) να αρνηθεί να ικανοποιήσει την αίτηση.

3.6. Υπάρχει υποχρέωση του αιτούντος να συμμετάσχει στην πληροφόρηση;

Ναι, ακόμη και αν η υποχρέωση συνεργασίας αναφέρεται μόνο στην αιτιολογική έκθεση 63, στη βιβλιογραφία που έχει δημοσιευθεί μέχρι σήμερα θεωρείται κυρίως ότι υπάρχει (όπως αναγνωρίστηκε στην Αυστρία στο πλαίσιο του DSG 2000): «όταν ο υπεύθυνος επεξεργασίας επεξεργάζεται μια μεγάλη ποσότητα πληροφοριών σχετικά με το υποκείμενο των δεδομένων, πρέπει να είναι εις θέσιν να ζητήσει, πριν από την παροχή των πληροφοριών, από το υποκείμενο των δεδομένων να προσδιορίσει τις πληροφορίες ή τις δραστηριότητες επεξεργασίας στις οποίες αναφέρεται η αίτηση».[3]

3.7. Τα δικαιώματα τρίτων πρέπει να λαμβάνονται υπόψη κατά την παροχή πληροφοριών;

Ναι, σύμφωνα με το Άρθρο 15 (4) του ΓΚΠΔ, το δικαίωμα παραλαβής αντιγράφου δεν μπορεί να επηρεάσει τα δικαιώματα και τις ελευθερίες των άλλων. Επιπλέον, στην αιτιολογική έκθεση 63 αναφέρεται ότι «το δικαίωμα δεν θα πρέπει να θίγει τα δικαιώματα ή τις ελευθερίες των άλλων, συμπεριλαμβανομένου του εμπορικού απορρήτου ή της πνευματικής ιδιοκτησίας, και ιδίως της πνευματικής ιδιοκτησίας που προστατεύει το

[2] See e.g. the jurisprudence of the Austrian High Courts: VwGH 4.7.2016, Ra 2016/04/0014; OGH 25.2.1993, 6 Ob 6/93)

[3] Recital 63.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

λογισμικό. Αποτέλεσμα, ωστόσο, αυτών των εκτιμήσεων δεν θα πρέπει να είναι η άρνηση παροχής όλων των πληροφοριών στο υποκείμενο των δεδομένων».

Είναι συνεπώς απαραίτητο να ελέγχονται τα αποκαλυπτόμενα δεδομένα, κατά κανόνα τα προσωπικά δεδομένα τρίτων (για παράδειγμα, το όνομα του προσώπου που διαχειρίζεται τον πελάτη και αναφέρεται στο αρχείο πελατών) πρέπει να διαγράφονται από το αντίγραφο των δεδομένων.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

4. Λίστα ελέγχου για την παροχή πληροφοριών κατόπιν αιτήσεως

Είμαι υποχρεωμένος να παράσχω πληροφορίες;	Εάν η δημόσια τοπική αρχή είναι υπεύθυνος επεξεργασίας δεδομένων - ΝΑΙ. Εάν η δημόσια τοπική αρχή είναι απλώς υπεύθυνος επεξεργασίας, αλλά εξακολουθεί να λαμβάνει αίτηση, πρέπει να την διαβιβάσει αμέσως στον υπεύθυνο.
Έλεγχος ταυτότητας	Η ταυτότητα του προσώπου που ζητεί τις πληροφορίες (του ενδιαφερομένου) πρέπει να είναι σαφής. Σε περίπτωση αμφιβολίας για την ταυτότητα: Ζητήστε απόδειξη.
Η παροχή των πληροφοριών είναι δωρεάν;	Καταρχήν - ΝΑΙ. Εάν ο αιτών έλαβε συχνά τις ίδιες πληροφορίες ή η αίτηση υπονομεύει σοβαρά τον υπεύθυνο επεξεργασίας, είναι πιθανό να προβλεφθεί τέλος. Προσοχή! Αυτό είναι επίσης θέμα εθνικής δικαιοδοσίας. Επομένως, ελέγξτε την ισχύουσα νομοθεσία σχετικά με τη δραστηριότητά σας.
Υπάρχουν καθόλου προσωπικά δεδομένα του αιτούντος που υποβάλλονται σε επεξεργασία;	Εάν δεν έχουν αποθηκευτεί δεδομένα σχετικά με τον αιτούντα ή εάν τα δεδομένα έχουν ήδη διαγραφεί ή τα δεδομένα έχουν αμετάκλητα καταστεί ανώνυμα, δεν θα γίνει επεξεργασία προσωπικών δεδομένων και θα παρασχεθούν οι αποκαλούμενες αρνητικές πληροφορίες - "Δεν επεξεργαζόμαστε δεδομένα σχετικά με εσάς".
Ποια δεδομένα και πληροφορίες πρέπει να παρέχει ο υπεύθυνος επεξεργασίας;	Πρέπει να παρέχονται όλα τα δεδομένα που αποθηκεύονται από τον ενδιαφερόμενο. Ανάλογα με την πολυπλοκότητα των συστημάτων, πρέπει να εξεταστεί εκ των προτέρων (από την άποψη του καταλόγου επεξεργασίας) σε ποια συστήματα ποιας κατηγορίας μπορούν να βρεθούν τα δεδομένα της

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

	κατηγορίας των επηρεαζομένων ατόμων. Επιπλέον, πρέπει να παρέχονται οι πληροφορίες που αναφέρονται στο Άρθρο 15 (1) του ΓΚΠΔ. Πρέπει να τηρούνται τα δικαιώματα τρίτων (κυρίως τα εμπορικά μυστικά και τα δεδομένα τρίτων πρέπει να διαγραφούν).

4.1. Έκδοση των πληροφοριών

Παράδειγμα παροχής πληροφοριών σύμφωνα με το Άρθρο 15 του ΓΚΠΔ

Η αίτησή σας για πληροφορίες

Αγαπητέ Κύριε / Κυρία [όνομα],

1. Η αίτησή σας από [ημερομηνία] για πληροφορίες σύμφωνα με το Άρθρο 15 ΓΚΠΔ, που ελήφθη από εμάς την [ημερομηνία], μπορεί να απαντηθεί ως εξής:

2. [Σε περίπτωση απάντησης μέσα σε διάστημα ενός μηνός από την παραλαβή] Με το παρόν επιβεβαιώνουμε εγκαίρως ότι επεξεργαζόμαστε τα προσωπικά δεδομένα σχετικά με εσάς.

[σε περίπτωση επέκτασης σύμφωνα με το Άρθρο 12 (3) ΓΚΠΔ] Όπως αναφέρεται στην επιστολή της [ημερομηνίας], αδράξαμε την ευκαιρία να παρατείνουμε την προθεσμία σε τρεις μήνες λόγω [της πολυπλοκότητας της αίτησης ή του αριθμού των αιτημάτων σας, περαιτέρω επεξηγήσεις είναι απαραίτητες].

3. [αν δεν έχει γίνει επεξεργασία δεδομένων] Δεν θα γίνει καμία επεξεργασία δεδομένων προσωπικού χαρακτήρα. [Έπειτα συνεχίστε με το text module αριθ. 9].

[Όταν έχει γίνει επεξεργασία δεδομένων] Συγκεκριμένα, επεξεργαζόμαστε τα ακόλουθα δεδομένα για εσάς: [εδώ είναι μια λίστα με τα πραγματικά δεδομένα που θα τύχουν επεξεργασίας].

Οι εκτυπώσεις / αντίγραφα από τη σχετική επεξεργασία δεδομένων βρίσκονται στο παράρτημα. Οποιαδήποτε παράλειψη έχει γίνει προκειμένου να μην επηρεαστούν τα δικαιώματα και οι ελευθερίες άλλων ή επειδή οι πληροφορίες δεν αφορούν εσάς ή τα προσωπικά σας στοιχεία.

4. [εάν τα δεδομένα δεν συλλέχθηκαν από το υποκείμενο των δεδομένων]: Λάβαμε τα δεδομένα σας από [διαθέσιμες πληροφορίες σχετικά με την προέλευση των δεδομένων σας, π.χ. δημόσιο φορέα ΧΨ].

5. [αν ισχύει] Θα χρησιμοποιήσουμε αυτοματοποιημένες διαδικασίες λήψης αποφάσεων / προφίλ που έχουν νομική ισχύ για εσάς ή θα σας επηρεάσουν κατά παρόμοιο τρόπο: [συμπληρώστε σημαντικές πληροφορίες όσον αφορά σ τη σχετική λογική και τις συνέπειες].

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

6. Έχετε τα δικαιώματα για διόρθωση, διαγραφή, περιορισμό και το δικαίωμα να αρνηθείτε την επεξεργασία των προσωπικών σας δεδομένων. Για τον λόγο αυτόν, επικοινωνήστε μαζί μας. Εάν πιστεύετε ότι η επεξεργασία των δεδομένων σας παραβιάζει το νόμο περί προστασίας δεδομένων ή εάν οι αξιώσεις προστασίας δεδομένων σας έχουν παραβιαστεί κατά κάποιον τρόπο, μπορείτε να διατυπώσετε υποβολή παραπόνων στην εποπτική αρχή. Σε αυτή τη χώρα, το ΧΨΩ είναι υπεύθυνο.

Θερμούς χαιρετισμούς

….

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

5. Εξωτερικές πηγές & Διαδικτυακοί Σύνδεσμοι

5.1. Βιβλία και άρθρα

- Souhrada-Kirchmayer, The right of access to the DSGVO, in Jahnel [Hrsg], Yearbook 17. Data Protection Law [2017] 86 f.
- ***Martini in Paal/Pauly*** (Ed.), Datenschutz-Grundverordnung (2016).

5.2. Άλλα έγγραφα και υποθέσεις

- jurisprudence of the Austrian High Courts: VwGH 4.7.2016, Ra 2016/04/0014; OGH 25.2.1993, 6 Ob 6/93) Web Links
- To compare the changes to directive 95/46/EC see https://gdpr.report/news/2017/11/20/gdpr-subject-access-requests/

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

ProLegis

Personas datu apstrādes juridiskais pamats

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

ProLegis

Saturs

1. TIESISKAIS REGULĒJUMS 4
   1.1. ES Pamattiesību harta 4
   1.2. Vispārīgā datu aizsardzības regula (VDAR) 4
2. JURIDISKAIS PAMATS PERSONAS DATU APSTRĀDEI SASKAŅĀ AR VDAR 10
   2.1. Piekrišana 10
      2.1.1. Nozīme un tiesiskās prasības 10
      2.1.2. Piemērojamība vietējo pašvaldību darbības kontekstā 12
   2.2. Līguma izpilde/ noslēgšana ar datu subjektu 13
      2.2.1. Nozīme un tiesiskās prasības 13
      2.2.2. Piemērojamība vietējo pašvaldību darbības kontekstā 14
   2.3. Juridisks pienākums (saistības) 14
      2.3.1. Nozīme un tiesiskās prasības 14
   2.4. Vitālās (būtiskas) intereses 16
      2.4.1. Nozīme un tiesiskās prasības 16
      2.4.2. Piemērojamība vietējo pašvaldību darbības kontekstā 16
   2.5. Uzdevums, kas tiek veikts sabiedrības interesēs vai īstenojot oficiālas pilnvaras 17
      2.5.1. Nozīme un tiesiskās prasības 17
      2.5.2. Piemērojamība vietējo pašvaldību darbības kontekstā 17
   2.6. Leģitīmās (likumiskās) intereses 18
      2.6.1. Nozīme un tiesiskās prasības 18
      2.6.2. Piemērojamība vietējo pašvaldību darbības kontekstā 19
3. SECINĀJUMI UN PRAKTISKIE PADOMI 19
4. ĀRĒJIE AVOTI UN TĪMEKĻA VIETNES 20

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

Grāmatas 20

29.panta darba grupas dokumenti 20

Tīmekļa saites 20

5. ATSAUCES ***21***

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

1. TIESISKAIS REGULĒJUMS

1.1. ES Pamattiesību harta

8.pants

Personas datu aizsardzība

1. Ikvienai personai ir tiesības uz savu personas datu aizsardzību.

*2. Šādi dati ir jāapstrādā godprātīgi, noteiktiem mērķiem un **ar attiecīgās personas piekrišanu vai ar citu likumīgu pamatojumu, kas paredzēts tiesību aktos**. Ikvienam ir pieejas tiesības datiem, kas par viņu savākti, un tiesības ieviest labojumus šajos datos.*

3. Atbilstību šiem noteikumiem kontrolē neatkarīga iestāde.

1.2. Vispārīgā datu aizsardzības regula (VDAR)

42.apsvērums

[…] Lai piekrišanu būtu apzināta, datu subjektam vajadzētu būt informētam vismaz par pārziņa identitāti un paredzētās personas datu apstrādes nolūkiem. Piekrišana nebūtu uzskatāma par brīvi izteiktu, ja datu subjektam nav īstas vai brīvas izvēles, vai viņš nevar atteikties vai atsaukt savu izvēli bez nelabvēlīgām sekām.

43.apsvērums

*Lai nodrošinātu, ka piekrišana ir sniegta brīvi, piekrišanai nevajadzētu kalpot par derīgu juridisko pamatu personas datu apstrādei konkrētā gadījumā, kad datu subjekta un pārziņa attiecībās pastāv skaidra nevienlīdzība, **jo īpaši, ja pārzinis ir publiska iestāde** un tāpēc ir maz ticams, ka piekrišana visos minētās konkrētās situācijas apstākļos bija sniegta brīvi. Uzskata, ka piekrišana nav sniegta brīvi, ja tā neparedz atsevišķu piekrišanu dažādām personas datu apstrādes darbībām, neraugoties uz to, ka tas ir atbilstīgi konkrētajā gadījumā, vai ja tiek noteikts, ka no šīs piekrišanas ir atkarīga līguma izpilde, tostarp pakalpojuma sniegšana, neraugoties uz to, ka minētā piekrišana nav noteikti nepieciešama šādai izpildei.*

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

44.apsvērums

Apstrādei vajadzētu būt likumīgai, ja tas ir ***nepieciešams saistībā ar līgumu vai nodomu noslēgt līgumu.***

45.apsvērums

Ja apstrādi veic saskaņā ar uz pārzini attiecināmu ***juridisku pienākumu****, vai ja apstrāde ir nepieciešama, lai izpildītu uzdevumu, ko veic sabiedrības interesēs vai īstenojot oficiālas pilnvaras, apstrādes pamatam vajadzētu būt noteiktam Savienības vai dalībvalsts tiesību aktos. Šajā regulā katrai atsevišķai apstrādei nav prasīts konkrēts tiesību akts. Var pietikt ar tiesību aktu, uz ko balstās vairākas apstrādes darbības, pamatojoties uz juridisku pienākumu, kas pārzinim jāpilda, vai ja apstrāde ir nepieciešama, lai izpildītu uzdevumu, ko veic sabiedrības interesēs vai īstenojot oficiālas pilnvaras. Arī apstrādes nolūkam vajadzētu būt noteiktam Savienības vai dalībvalstu tiesību aktos. Turklāt minētajā tiesību aktā varētu precizēt vispārējos nosacījumus, kas paredzēti šajā regulā, kura reglamentē personas datu apstrādes likumīgumu, izstrādāt norādes, kā noteikt pārzini, apstrādājamo personas datu veidu, attiecīgos datu subjektus, vienības, kurām personas dati var tikt izpausti, apstrādes nolūka ierobežojumus, glabāšanas laikposmu un citus pasākumus, lai nodrošinātu likumīgu un godprātīgu apstrādi. Tāpat Savienības vai dalībvalstu tiesību aktos būtu jānosaka, vai pārzinim, kurš pilda uzdevumu, ko veic sabiedrības interesēs vai īstenojot oficiālas pilnvaras, vajadzētu būt publiskai iestādei vai citai fiziskai vai juridiskai personai, kas ir publisko tiesību subjekts vai – ja tas ir sabiedrības interesēs, tostarp veselības nolūkos, piemēram, sabiedrības veselība, sociālā aizsardzība un veselības aprūpes pakalpojumu pārvaldība – privāttiesību subjekts, kā, piemēram, profesionāla apvienība.*

46.apsvērums

Personas datu apstrāde būtu jāuzskata par likumīgu arī tad, ja tā nepieciešama, lai aizsargātu ***intereses, kas ir būtiski svarīgas datu subjekta vai citas fiziskas personas dzīvei****. Personas datu apstrādei, pamatojoties uz citas fiziskās personas vitālajām interesēm, principā būtu jānotiek tikai tad, ja apstrādi nevar acīmredzami balstīt uz citu juridisko pamatu. Dažus apstrādes veidus var izmantot, pamatojoties gan uz svarīgām sabiedrības interesēm, gan uz datu subjekta vitālajām interesēm, piemēram, ja apstrāde ir vajadzīga humanitāros nolūkos,*

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

tostarp epidēmiju un to izplatīšanās monitoringam vai ārkārtas humanitārajās situācijās, jo īpaši dabas un cilvēka izraisītu katastrofu situācijās.

47. apsvērums

Pārziņa, tostarp tāda pārziņa, kuram personas dati var tikt izpausti, vai trešās personas leģitīmās intereses *var būt apstrādes juridiskais pamats ar noteikumu, ka datu subjekta intereses vai pamattiesības un pamatbrīvības nav svarīgākas, ņemot vērā saprātīgas datu subjektu gaidas, kuru pamatā ir viņu attiecības ar pārzini. Šādas leģitīmas intereses varētu būt, piemēram, tad, ja starp datu subjektu un pārzini pastāv būtiskas un atbilstošas attiecības, piemēram, ja datu subjekts ir pārziņa klients vai ir pārziņa dienestā. Jebkurā gadījumā būtu rūpīgi jāizvērtē, vai pastāv leģitīmas intereses, tostarp, vai datu subjekts personas datu vākšanas laikā un saistībā ar to var pamatoti sagaidīt, ka var notikt minētajā nolūkā paredzēta apstrāde. Datu subjekta intereses un pamattiesības varētu būt svarīgākas par datu pārziņa interesēm, ja personas datus apstrādā apstākļos, kādos datu subjektiem nav pamatotu gaidu, ka apstrāde turpināsies. Ņemot vērā, ka personas datu apstrādes juridiskais pamats publiskām iestādēm ar likumu ir jānosaka likumdevējam, minētais juridiskais pamats nebūtu jāpiemēro apstrādei, ko veic publiskas iestādes, pildot savus uzdevumus. Personas datu apstrāde tikai tādā apjomā, kas vajadzīgs, lai novērstu krāpšanu, arī ir attiecīgā datu pārziņa leģitīmās interesēs. Var uzskatīt, ka personas datu apstrāde tiešās tirgvedības vajadzībām ir veikta leģitīmās interesēs.*

48.apsvērums

Pārziņiem, kas ir uzņēmumu grupas daļa vai kādai centrālai struktūrai radniecīgas iestādes, var būt leģitīmas intereses personas datus nosūtīšanā citiem grupas uzņēmumiem iekšējos administratīvos nolūkos, tostarp klientu vai darba ņēmēju personas datu apstrādei. Neskarti saglabājas vispārējie principi par uzņēmumu grupas iekšienē veiktu personas datu nosūtīšanu kādam uzņēmumam, kas atrodas trešā valstī.

49.apsvērums

Attiecīgā datu pārziņa leģitīmas intereses rada personas datu apstrāde, kuru veic publiskas iestādes, Datorapdraudējumu reaģēšanas vienības (CERT), Datordrošības incidentu reaģēšanas vienības (CSIRT), elektronisko sakaru tīklu un pakalpojumu sniedzēji un drošības tehnoloģiju un pakalpojumu sniedzēji, tādā apjomā, kas ir noteikti vajadzīgs un

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

samērīgs, lai nodrošinātu tīkla un informācijas drošību, t. i., tīkla vai informācijas sistēmu spēju zināmā uzticamības līmenī pretoties nejaušiem gadījumiem vai nelikumīgām vai ļaunprātīgām darbībām, kas apdraudētu uzglabāto un nosūtīto personas datu pieejamību, autentiskumu, integritāti un konfidencialitāti, kā arī saistīto pakalpojumu drošību, kurus piedāvā minētie tīkli un sistēmas vai kuri ir pieejami, izmantojot minētos tīklus un sistēmas. Tas varētu, piemēram, palīdzēt novērst neatļautu piekļuvi elektroniskajiem sakaru tīkliem un ļaunprātīgu kodu izplatīšanu, kā arī apturēt pakalpojumatteices uzbrukumus un novērst datoru un elektronisko komunikāciju sistēmu bojājumus.

50.apsvērums

Personas datu apstrāde nolūkos, kas nav tie, kādos personas dati sākotnēji tika vākti, būtu jāatļauj tikai tad, ja apstrāde ir saderīga ar tiem nolūkiem, kādos personas dati sākotnēji tika vākti. Šādā gadījumā nav vajadzīgs atsevišķs juridiskais pamats kā vien tas, ar ko tika atļauta personas datu vākšana. Ja apstrāde ir vajadzīga, lai izpildītu uzdevumu, ko veic sabiedrības interesēs vai īstenojot pārzinim likumīgi piešķirtās oficiālās pilnvaras, Savienības vai dalībvalsts tiesību aktos var būt noteikti un precizēti uzdevumi un nolūki, kādos turpmākā apstrāde būtu jāuzskata par saderīgu un likumīgu. Turpmākā apstrāde arhivēšanas nolūkos sabiedrības interesēs, zinātniskās vai vēstures pētniecības nolūkos, vai statistikas nolūkos būtu jāuzskata par saderīgām likumīgām apstrādes darbībām. Personas datu apstrādes juridiskais pamats, ko paredz Savienības vai dalībvalsts tiesību akti, var arī paredzēt juridisko pamatu turpmākai apstrādei. Lai pārliecinātos, vai turpmākas apstrādes nolūks ir saderīgs ar nolūku, kādā personas dati sākotnēji tika vākti, pārzinim – pēc tam, kad ir izpildītas visas prasības attiecībā uz sākotnējās apstrādes likumīgumu, – būtu cita starpā jāņem vērā: jebkura saikne starp minētajiem nolūkiem un paredzētās turpmākās apstrādes nolūkiem; konteksts, kādā personas dati ir vākti, jo īpaši saprātīgas datu subjektu gaidas, kuru pamatā ir to attiecības ar pārzini, attiecībā uz datu turpmāku izmantošanu; personas datu raksturs; sekas, ko paredzētā turpmākā apstrāde rada datu subjektiem; un atbilstošu garantiju esamība gan sākotnējās, gan paredzētajās turpmākās apstrādes darbībās.

Ja datu subjekts ir devis piekrišanu vai ja apstrāde balstās uz Savienības vai dalībvalsts tiesību aktiem, kas demokrātiskā sabiedrībā ir vajadzīgs un samērīgs pasākums, lai jo īpaši aizsargātu svarīgus vispārējo sabiedrības interešu mērķus, būtu jāļauj pārzinim turpināt personas datu apstrādi neatkarīgi no saderības ar nolūkiem. Jebkurā gadījumā būtu jānodrošina, lai tiktu piemēroti šajā regulā noteiktie principi un jo īpaši lai datu subjekts tiktu informēts par minētajiem citiem apstrādes nolūkiem un

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

par savām tiesībām, tostarp par tiesībām iebilst. Būtu jāuzskata, ka pārziņa leģitīmajās interesēs ir tas, ka pārzinis norāda uz iespējamām noziedzīgām darbībām vai uz draudiem sabiedriskajai drošībai un atsevišķos gadījumos vai vairākos gadījumos, kas saistīti ar vienu un to pašu noziedzīgo darbību vai vieniem un tiem pašiem draudiem sabiedriskajai drošībai, nosūta attiecīgos personas datus kompetentai iestādei. Tomēr šāda nosūtīšana pārziņa leģitīmajās interesēs vai turpmāka personas datu apstrāde būtu jāaizliedz, ja apstrāde nav saderīga ar juridisku, profesionālu vai citu saistošu pienākumu ievērot dienesta noslēpumus.

4.pants

Definīcijas

Šajā regulā:

[…]

(11) datu subjekta "piekrišana" ir jebkura ***brīvi sniegta, konkrēta, apzināta un viennozīmīga norāde uz datu subjekta vēlmēm, ar kuru viņš paziņojuma vai skaidri apstiprinošas darbības veidā sniedz piekrišanu savu personas datu apstrādei****;*

6.pants

Apstrādes likumīgums

1. Apstrāde ir likumīga tikai tādā apmērā un tikai tad, ja ir ***piemērojams vismaz viens no turpmāk minētajiem pamatojumiem:***

(a) datu subjekts ir devis piekrišanu savu personas datu apstrādei vienam vai vairākiem konkrētiem nolūkiem;

(b) apstrāde ir vajadzīga līguma, kura līgumslēdzēja puse ir datu subjekts, izpildei vai pasākumu veikšanai pēc datu subjekta pieprasījuma pirms līguma noslēgšanas;

(c) apstrāde ir vajadzīga, lai izpildītu uz pārzini attiecināmu juridisku pienākumu;

(d) apstrāde ir vajadzīga, lai aizsargātu datu subjekta vai citas fiziskas personas vitālas intereses;

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

(e) apstrāde ir vajadzīga, lai izpildītu uzdevumu, ko veic sabiedrības interesēs vai īstenojot pārzinim likumīgi piešķirtās oficiālās pilnvaras;

(f) apstrāde ir vajadzīga pārziņa vai trešās personas leģitīmo interešu ievērošanai, izņemot, ja datu subjekta intereses vai pamattiesības un pamatbrīvības, kurām nepieciešama personas datu aizsardzība, ir svarīgākas par šādām interesēm, jo īpaši, ja datu subjekts ir bērns.

Pirmās daļas f) apakšpunktu nepiemēro apstrādei, ko veic publiskas iestādes, pildot savus uzdevumus.

2. Dalībvalstis var paturēt spēkā vai ieviest konkrētākus noteikumus, lai šīs regulas noteikumu piemērošanu pielāgotu attiecībā uz apstrādi, ko veic, lai ievērotu 1. punkta c) un e) apakšpunktu, nosakot precīzāk konkrētas prasības apstrādei un citus pasākumus, ar ko nodrošina likumīgu un godprātīgu apstrādi, tostarp citās konkrētās apstrādes situācijās, kas paredzētas IX nodaļā.

3. Šā panta 1. punkta c) un e) apakšpunktā minēto apstrādes pamatu nosaka ar:

(a) Savienības tiesību aktiem; vai

(b) dalībvalsts tiesību aktiem, kas piemērojami pārzinim.

Apstrādes nolūku nosaka minētajā juridiskajā pamatā vai – attiecībā uz 1. punkta e) apakšpunktā minēto apstrādi – tas ir vajadzīgs, lai izpildītu uzdevumu, ko veic sabiedrības interesēs vai īstenojot pārzinim likumīgi piešķirtās oficiālās pilnvaras. Minētajā juridiskajā pamatā var būt ietverti konkrēti noteikumi, lai pielāgotu šīs regulas noteikumu piemērošanu, cita starpā vispārēji nosacījumi, kas reglamentē pārziņa īstenotu apstrādes likumību; apstrādājamo datu veidi; attiecīgie datu subjekti; vienības, kurām personas dati var tikt izpausti, un mērķi, kādiem tie var tikt izpausti; apstrādes nolūka ierobežojumi; glabāšanas termiņi; un apstrādes darbības un apstrādes procedūras, tostarp pasākumi, lai nodrošinātu likumīgu un godprātīgu apstrādi, piemēram, citās konkrētās datu apstrādes situācijās, kas paredzētas IX nodaļā. Savienības vai dalībvalsts tiesību akti atbilst sabiedrības interešu mērķim un ir samērīgi ar izvirzīto leģitīmo mērķi.

4. Ja apstrāde citā nolūkā nekā tajā, kādā personas dati tika vākti, nav balstīta uz datu subjekta piekrišanu vai uz Savienības vai dalībvalsts tiesību aktiem, kas demokrātiskā sabiedrībā ir vajadzīgs un samērīgs pasākums, lai aizsargātu 23. panta 1. punktā minētos mērķus, pārzinis, lai pārliecinātos, vai apstrāde citā nolūkā ir savietojama ar nolūku, kādā personas dati sākotnēji tika vākti, cita starpā ņem vērā:

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

(a) jebkuru saikni starp nolūkiem, kādos personas dati ir vākti, un paredzētās turpmākās apstrādes nolūkiem;

(b) kontekstu, kādā personas dati ir vākti, jo īpaši saistībā ar datu subjektu un pārziņa attiecībām;

(c) personas datu raksturu, jo īpaši to, vai ir apstrādātas īpašas personas datu kategorijas, ievērojot 9. pantu, vai to, vai ir apstrādāti personas dati, kas attiecas uz sodāmību un pārkāpumiem, ievērojot 10. pantu;

(d) paredzētās turpmākās apstrādes iespējamās sekas datu subjektiem;

(e) atbilstošu garantiju esamību, kas var ietvert šifrēšanu vai pseidonimizāciju.

2. JURIDISKAIS PAMATS PERSONAS DATU APSTRĀDEI SASKAŅĀ AR VDAR

2.1. Piekrišana

2.1.1. Nozīme un tiesiskās prasības

Piekrišana ir viens no sešiem juridiskajiem pamatiem, kas uzskaitīti VDAR 6.pantā. Lai piekrišana būtu derīga, VDAR paredz, ka tā ir brīvi sniegta, konkrēta, informēta (apzināta) un vienozīmīga.

- **"brīvi"** = datu subjektiem nozīmē reālu izvēli un kontroli[1]. Ja datu subjektam rodas jebkādas nelabvēlīgas sekas gadījumā, ja viņš nepiekrīt savu datu apstrādei vai atsakās no jau dotas piekrišanas (piemēram, pakalpojuma atteikums, lielākas preču/pakalpojumu izmaksas - maksa, cena utt.), uzskatāms, ka piekrišana nav brīvi dota. Sakarā ar pilnvaru nesamērību starp publiskām iestādēm un datu subjektiem, piekrišana būtu reti noderīgs datu apstrādes līdzeklis oficiālo pilnvaru izpildē;
- **"konkrēta"** = cieši saistīts ar prasību, ka datu subjekts piekrīt vienam vai vairākiem konkrētiem datu apstrādes mērķiem (tā dēvētā piekrišanas "granularitāte"[2]), un mērķa specifikācijas principu. Katram no datu apstrādes mērķiem ir jābūt skaidri definētam no paša sākuma pirms datu subjekta piekrišanas. Datu subjektam jābūt iespējai izvēlēties, kādiem datu apstrādes mērķiem piekrist (piemēram, dot piekrišanu nolūkam A, B un C, nevis dod piekrišanu nolūkam E un D). Informācijai, kas saistīta ar piekrišanu, jābūt skaidri nošķirtai no informācijas, kas saistīta ar citiem jautājumiem. Jebkuram jaunam apstrādes mērķim ir jāsaņem jauna

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

piekrišana, un pārzinim jāsniedz konkrēta informācija katrā atsevišķā piekrišanas pieprasījumā par datiem, kas tiek apstrādāti katram mērķim;

- **"informēta" (“apzināta”)** = VDAR minimālās prasības paredz, ka datu pārzinis sniedz datu subjektam informāciju par datu apstrādi un tās mērķiem. 29.panta darba grupa (DG29) iesaka iekļaut papildu informāciju, piemēram, par savākto un izmantoto datu veidu; tiesībām atsaukt piekrišanu; informāciju par datu izmantošanu tādiem lēmumiem, kuru pamatā ir tikai automatizēta apstrāde, tostarp profilēšana[3]; datu pārsūtīšanas gadījumā - informācija par iespējamiem riskiem saistībā ar datu pārsūtīšanu trešajām valstīm, ja nav pieņemts lēmums par atbilstību un nav nodrošināti piemēroti aizsardzības pasākumi[4];
- **"viennozīmīga"** = datu subjektam piekrišana jāsniedz paziņojuma vai skaidri apstiprinošas darbības veidā. Piekrišana vienmēr jādod, izmantojot aktīvu rīcību vai deklarāciju. Tādējādi klusēšana, iepriekš atzīmēta ailīte un neaktivitāte nevar būt derīga piekrišana saskaņā ar VDAR;
- **Tikpat viegli atsaucama, kā sniegta** = piekrišana var tikt atsaukta jebkurā laikā. Tas nav obligāti veicams ar tādu pašu darbību, bet atteikšanās procesam jābūt tikpat vienkāršam kā piekrišanas procesam (piemēram, noklikšķinot uz lodziņa tiešsaistes deklarācijā, lai piekristu saņemt pašvaldības avīzi, ir tikpat viegli, kā noklikšķinot uz saites e-pasta ziņojumā, kas pievienots biļetenam, par abonēšanas anulēšanu un piekrišanas atsaukšanu);
- **Īpašas prasības attiecībā uz bērnu piekrišanu** = VDAR uzlūko bērnus kā neaizsargātu datu subjektu kategoriju. Tādēļ viņiem nepieciešama īpaša aizsardzība, jo viņi var mazāk apzināties attiecīgos riskus, sekas, aizsardzības pasākumus un savas tiesības saistībā ar personas datu apstrādi. Tādā gadījumā, kad bērnam tiek sniegti informācijas sabiedrības pakalpojumi (piemēram, tiešsaistes izglītības kampaņas pašvaldību tīmekļa vietnē, kur nepieciešams savākt bērnu datus), bērnu vecumā līdz 16 gadiem piekrišanu datu apstrādei (dalībvalstis var samazināt šo vecuma slieksni līdz 13 gadiem) dod vai apstiprina persona, kurai ir vecāku atbildība par bērnu;
- **Piekrišana saskaņā ar Direktīvu 95/46** = iepriekšējā sistēmā iegūtā piekrišana nav obligāti jāiegūst no jauna. Ja piekrišana atbilst VDAR noteiktajām prasībām, tad piekrišana, kas iegūta saskaņā ar direktīvu, arī turpmāk uzskatāma par derīgu apstrādes pamatu.

Datu pārziņa pienākums ir spēt pierādīt, ka piekrišana ir pienācīgi iegūta[5].

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

2.1.2. *Piemērojamība vietējo pašvaldību darbības kontekstā*

Praksē piekrišana reti būs primārais juridiskais pamats vietējo pašvaldību likumīgai iedzīvotāju personas datu apstrādei. Šis secinājums izriet no VDAR prasībām, kurām piekrišanai jāatbilst, lai tā būtu derīga.

Pirmkārt, fakts, ka piekrišana ir "jādod brīvi", t.i., datu subjektam nevajadzētu radīt nelabvēlīgas sekas gadījumā, ja netiek dota piekrišana, nozīmē, ka jebkurā situācijā, kurā konkrēta pašvaldība darbojas kā publiskās varas turētājs, piekrišana nevar tikt izmantota kā derīgs juridiskais pamats datu apstrādei. Kontrole par iedzīvotāju pienācīgu sabiedrisko pienākumu izpildi (piemēram, vietējo nodevu un nodokļu iekasēšana, nekustamo īpašumu reģistrācija utt.) un sankciju piemērošana šādu saistību neizpildes gadījumā ir saistīta ar tiesībām (un pienākumiem) izmantot piespiedu pilnvaras. Tas nozīmē, ka datu subjektiem nav reālas brīvas izvēles, lai piekristu vai nepiekristu viņu personas datu apstrādei. Tie atrodas pakļautībā un saskaņā ar likumu tiem ir pienākums sadarboties ar pašvaldību.

Otrkārt, piekrišanu var atsaukt "jebkurā brīdī". Ja personām, pildot savas juridiskās saistības, piekrišana būtu personas datu apstrādes likumīgais pamats, tad potenciāli jebkura persona, kas rīkojas ļaunprātīgi (piemēram, nevēlas pildīt noteiktus sabiedriskos pienākumus), var jebkurā brīdī atsaukt savu piekrišanu un, izmantojot šo atsaukumu, radīt šķēršļus (un praksē "bloķēt") pašvaldības normālu darbību. Ja piekrišana ir atsaukta, pašvaldībai kā datu pārzinim jāpārtrauc datu apstrāde. Tas ir neiedomājami, pildot oficiālās pilnvaras, jo tas apdraudētu visu ideju par publiskās varas izmantošanu.

Tādējādi iepriekš aprakstītajās situācijās piekrišana nav piemērots rīks šādai datu apstrādei.

Balstoties uz DG29, "saskaņā ar VDAR tiesisko regulējumu piekrišanas izmantošana likumīgai datu apstrādei publiskām iestādēm **nav pilnībā izslēgta**"[6]. Tādējādi piekrišana varētu būt izmantojama situācijās, kad pašvaldība vai nu neizmanto savas tipiskās un galvenās funkcijas, vai arī attiecīgā apstrāde nav obligāta (un ir izveidotas noklusējuma apstrādes procedūras, kas tiek izmantotas, ja datu subjekts nav devis piekrišanu). Piemēri ir šādas situācijas:

- pašvaldība un valsts iestāde pieprasa vienu un to pašu informāciju kāda dokumenta sagatavošanā pēc personas pieprasījuma, bet nespēj piekļūt viena otras datu bāzēm. Tā kā abas iestādes personai pieprasa vienu un to pašu informāciju, tās var jautāt personas piekrišanu apvienot failus, lai izvairītos no divkāršas procedūras un sarakstes. Abām

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

publiskajām iestādēm jānodrošina, ka tas tomēr nav obligāti un ka dokumenta izdošana tiks nodrošināta pat, ja persona nepiekrīt datu apvienošanai[7];

- pašvaldība nodrošina iespēju informēt iedzīvotājus, kas piedalās administratīvajā procesā, izmantojot e-pastu. Pastāv izvēles režīms, t.i., iedzīvotāji var brīvi izlemt, vai saņemt paziņojumus e-pastā (piemēram, atzīmējot lodziņu tiešsaistes/papīra formā un norādot savu e-pastu). Piekrišanas atteikuma vai atsaukšanas gadījumā, pašvaldībai jāparedz cita paziņošanas procedūra (piemēram, ierakstīta vēstule). E-pasta apstrāde šādā gadījumā būtu balstīta uz piekrišanu;
- pašvaldība nodrošina iedzīvotājiem iespēju parakstīties ielūgumu saņemšanai dažādiem pašvaldības organizētiem pasākumiem (piemēram, izstādes vietējos muzejos, teātra priekšnesumi pašvaldības teātrī, atkritumu savākšanas kampaņas, konkursi, izglītības kampaņas skolās). Abonementam ir jānorāda kontaktinformācija (piemēram, pasta adrese, tālruņa numurs, e-pasts u.c.), kā arī informācija par datu subjekta vēlmēm (piemēram, par vaļaspriekiem, interesēm utt.). Šādu datu apstrāde būtu balstīta uz piekrišanu, jo iedzīvotājiem ir tiesības jebkurā laikā brīvi un bez nelabvēlīgām sekām atteikties no šādiem paziņojumiem.

2.2. Līguma izpilde/ noslēgšana ar datu subjektu

2.2.1. Nozīme un tiesiskās prasības

Nosacījumos, kas minēti VDAR 6.panta 1.punkta "b" apakšpunktā, aprakstīti divi **atsevišķi** juridiskie pamatojumi personas datu apstrādei:

(i) situācijas, kad apstrāde jāveic līguma, kurā datu subjekts ir līgumslēdzēja puse, izpildei;

(ii) situācijas, kad datu apstrāde notiek pirms līguma noslēgšanas. Tas ietver pirmslīgumiskās attiecības ar nosacījumu, ka pasākumi ir veikti pēc datu subjekta pieprasījuma, nevis pārziņa vai trešo personu iniciatīvas[8].

Pirmais noteikums ir jāinterpretē stingri, un tas neattiecas uz gadījumiem, kad apstrāde nav patiešām vajadzīga, lai izpildītu līgumu, bet gan to datu subjektam vienpusēji noteicis pārzinis[9]. Saskaņā ar DG29 sniegto interpretāciju par šo pašu juridisko pamatu vairs spēkā neesošajā Direktīvā 95/46, minētais juridiskais pamats attiecas tikai uz to, kas nepieciešams līguma **izpildei**. Citiem vārdiem sakot, kamēr datu apstrāde attiecas uz parastu līguma izpildi, tam par pamatu varētu būt šis juridiskais pamatojums. Šis pamats attiecas uz gadījumiem, kad apstrāde notiek līguma ietvaros, neatkarīgi no līguma izpildes posma[10]. Tomēr uz jebkādām turpmākajām darbībām, kuras izraisījusi neatbilstība vai cits atgadījums līguma izpildē, šis juridiskais pamats neattiecas. Šāda

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

veida apstrādei būtu jāpiemēro cits juridiskais pamats, piemēram, datu pārziņa leģitīmās (likumiskās) intereses.

Otrs noteikums varētu ietvert datu apstrādi, kas nepieciešama piedāvājumu sagatavošanai, personāla atlases darbam utt. Tomēr jebkāda detalizētāka kandidātu pagātnes pārbaude būtu plašāka un nebūtu attaisnojama kā datu subjekta pieprasītie pasākumi.

Parasti šo tiesisko pamatu regulatori interpretē šauri, tādēļ datu pārzinim jāspēj apliecināt, ka datu apstrāde ir neizbēgama līguma izpildei[11].

2.2.2. Piemērojamība vietējo pašvaldību darbības kontekstā

Šo personas datu apstrādes tiesisko pamatu pašvaldības var piemērot vismaz sekojošos gadījumos:

- Datu apstrāde nodarbinātības kontekstā – piemēram, algu informācijas un banku kontu datu apstrāde, lai varētu izmaksāt algas[12];
- Datu apstrāde saistībā ar publiskā iepirkuma līgumu slēgšanu - šis personas datu apstrādes līgumiskais tiesiskais pamats varētu pārklāties ar citu tiesisko pamatu - piemēram, pašvaldības juridisko pienākumu veikt personas datu apstrādi administratīvā procesa ietvaros, kas noteikts vietējos tiesību aktos;
- Datu apstrāde saistībā ar attiecībām starp uzņēmumu, kurš pilnībā vai daļēji pieder pašvaldībai vai valstij, un iedzīvotāju. Piemēram, slēdzot attiecīgus līgumus ar uzņēmumiem, kas sniedz sabiedriskā transporta pakalpojumus visā pilsētā/ novadā, vai uzņēmumiem, kas sniedz komunālos pakalpojumus (elektrības, gāzes, ūdensapgādes u.c.).

2.3. Juridisks pienākums (saistības)

2.3.1. Nozīme un tiesiskās prasības

Šim juridiskajam pamatam nepieciešams skaidrs tiesiskais regulējums, kas ieviests vai likumos, vai pakārtotajos normatīvajos aktos (tā dažās dalībvalstīs dēvē sekundāros tiesību aktus), kas uzliek par pienākumu datu pārzinim veikt apstrādi. DG29 uzsver: lai saistības būtu spēkā un tās būtu saistošas, tiesību aktam ir jāatbilst visiem attiecīgajiem nosacījumiem, un tam arī jāatbilst datu aizsardzības tiesību aktam, tostarp vajadzīguma, samērīguma un nolūka ierobežojuma prasībām[13]. VDAR skaidri nosaka, ka šim pienākumam kumulatīvi ir jābūt:

(i) pārziņa pienākumam, kas noteikts dalībvalsts vai ES tiesību aktā. Šajā sakarā DG29 saskaņā ar vairs spēkā neesošo Direktīvu 95/46 jau interpretējusi

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

sekojoši: pienākumi saskaņā ar trešo valstu likumiem (piemēram, pienākums izveidot pārkāpumu ziņošanas sistēmas saskaņā ar ASV 2002. gada likumu Sarbanes-Oxley) neietilpst tiesiskajā pamatā - juridisks pienākums. Lai tas būtu spēkā, trešās valsts juridiskajam pienākumam jābūt oficiāli atzītam un integrētam attiecīgās dalībvalsts tiesiskajā kārtībā, piemēram, starptautiska nolīguma veidā; un

(ii) "skaidram un precīzam", un tas ir saistošs personām, uz kurām tas attiecas. VDAR 41. un 45. apsvērumi skaidro, ka attiecīgajiem "juridiskajiem pienākumiem" nav jābūt likumā noteiktiem, kam varētu būt praktiskas sekas “common Law” (precedentu tiesībās balstītās) valstīs – būtu pietiekami, ja tas atbilst "skaidri un precīzi" testam. Juridiskais pienākums var attiekties uz vairākām datu apstrādes darbībām, kuras veic pārzinis, tāpēc var nebūt nepieciešams noteikt specifisku juridisku pienākumu attiecībā uz katru atsevišķu apstrādes darbību[14].

DG29 ir norādījusi: lai piemērotu šo juridisko pamatu, pārzinim nedrīkst būt izvēles brīvība pildīt vai nepildīt šo pienākumu. Šis juridiskais pamats neattiecas uz brīvprātīgām vienpusējām attiecībām un publiskām un privātām partnerībām, kurās datus apstrādā vairāk, nekā noteikts tiesību aktā[15]. Juridisks pienākums kā personas datu apstrādes pamats ir jāpiemēro, pamatojoties uz tiesību normām, kurās skaidri norādīts apstrādes veids un objekts. Pārzinim nedrīkst būt nesamērīga rīcības brīvība attiecībā uz tā juridisko saistību ievērošanu[16].

DG29 skaidri apstiprina, ka tiesību aktos dažkārt var būt noteikts tikai vispārējs mērķis, bet konkrētākas saistības ir noteiktas citā līmenī, piemēram, vai nu sekundāros tiesību aktos, vai ar valsts iestādes saistošu lēmumu konkrētā gadījumā. Saskaņā ar DG29 tas var arī radīt juridiskas saistības, ja apstrādes veids un objekts ir pienācīgi definēti un tiem piemērojams pienācīgs juridiskais pamats[17].

2.3.2. Piemērojamība vietējo pašvaldību darbības kontekstā

Praksē šim juridiskajam pamatam būtu jābūt vienam no nozīmīgākajiem juridiskajiem pamatiem pašvaldību veiktajā personas datu apstrādē. Šis juridiskais pamats attiektos gan uz situācijām, kas saistītas ar administratīvo pakalpojumu sniegšanu vai iedzīvotāju sabiedrisko pienākumu izpildes veicināšanu, gan uz situācijām, kas saistītas ar īpašu pašvaldības pienākumu pildīšanu darba devēja statusā. Šo juridisko pamatu varētu piemērot, piemēram, šādās situācijās:

- pašvaldība veic datu vākšanu, lai apstrādātu informāciju par naudas sodiem par automobiļu novietošanu neatļautās vietās;

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

- pašvaldība ziņo savu darbinieku algas datus sociālā nodrošinājuma vai nodokļu iestādēm[18].

2.4. Vitālās (būtiskas) intereses

2.4.1. Nozīme un tiesiskās prasības

Šis juridiskais pamats jāinterpretē ļoti šauri. DG29 arī atzinusi, ka vitālām interesēm jābūt ierobežotai piemērošanas jomai[19]. Jēdziens "vitālas intereses" pēc būtības ir saistīts ar nenovēršamu apdraudējumu datu subjekta pamatvajadzībām (dzīvība, veselība, ķermeņa veselums utt.). Tiesību doktrīnā norādīts, ka attiecīgajai datu apstrādei jābūt vitāli svarīgai indivīda izdzīvošanai[20]. Saskaņā ar DG29 interpretāciju vairs spēkā neesošās Direktīvas 95/46 ietvaros, draudiem ir jābūt **tūlītējiem**, t.i., liela apjoma personas datu vākšana un apstrāde tikai preventīviem nolūkiem nevar attiekties uz šo juridisko pamatu[21]. VDAR 46. apsvērums nepārprotami atļauj apstrādi, balstoties uz šo juridisko pamatu humanitāros nolūkos, tostarp epidēmiju un to izplatīšanās monitoringam vai ārkārtas humanitārajās situācijās, jo īpaši dabas un cilvēka izraisītu katastrofu situācijās (šajos scenārijos var būt divu būtisku juridisko pamatu pārklāšanās - sabiedrības intereses un vitālās intereses). Tādējādi šī striktā interpretācija, ko uzliek DG29, nākotnē varētu tikt "mīkstināta".

Jāatzīmē, ka saskaņā ar vairs spēkā neesošo Direktīvu 95/46 juridiskais pamats "vitālās intereses" attiecās tikai uz datu subjekta interesēm. VDAR šī juridiskā pamata darbības joma ir plašāka - vitālās intereses var būt gan datu subjektam, gan citai fiziskai personai. VDAR skaidri nosaka, ka personas datu apstrāde, pamatojoties uz citas fiziskas personas vitālajām interesēm, principā var notikt tikai tad, ja apstrādi nevar **acīmredzami** balstīt uz citu juridisko pamatu. Citiem vārdiem sakot, apstrādes pamatošana ar vitālām interesēm pārzinim būtu drīzāk pamatojuma "pēdējais līdzeklis".

2.4.2. Piemērojamība vietējo pašvaldību darbības kontekstā

Iespēja piemērot šo pamatu pašvaldību darbības kontekstā ir diezgan ierobežota. Šo juridisko pamatu teorētiski varētu piemērot ļoti ierobežotā skaitā gadījumu, piemēram, lai attaisnotu darbinieku vai iedzīvotāju personas datu apstrādi ārkārtas situācijās, kas radušās pašvaldību jurisdikcijā un ja nav cita juridiskā pamata šādai apstrādei (piemēram, juridisks pienākums vai oficiālo pilnvaru īstenošana).

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

2.5. Uzdevums, kas tiek veikts sabiedrības interesēs vai īstenojot oficiālas pilnvaras

2.5.1. Nozīme un tiesiskās prasības

Datu pārziņa uzdevumam vai pilnvarai būtu jābūt noteiktiem ES vai dalībvalsts tiesību aktos, kuri attiecas uz pārzini. Uzdevumi, kas tiek veikti kādas trešās valsts sabiedrības interesēs vai īstenojot piešķirtas oficiālās pilnvaras, kas piešķirtas saskaņā ar ārvalstu tiesību aktiem, neietilpst šā noteikuma piemērošanas jomā saskaņā ar vairs spēkā neesošo Direktīvu 95/46[22], un šī pieeja tiek turpināta arī VDAR.

Šī noteikuma analogs iepriekšējā direktīvā aptvēra divas dažādas situācijas:

(i) pārzinim ir oficiālas pilnvaras vai tas veic sabiedrības interesēs realizējamu uzdevumu (taču tam nav jābūt arī juridiskām saistībām apstrādāt datus) un kad apstrāde jāveic, lai īstenotu šīs pilnvaras vai veiktu minēto uzdevumu, vai

(ii) pārzinim nav oficiālu pilnvaru, taču tam pieprasa atklāt datus trešā persona, kurai ir šādas pilnvaras[23].

VDAR ir izņemts otrs kritērijs, t.i., situācijas, kad oficiālo pilnvaru īstenošana ir uzticēta personai, kurai dati tiek izpausti, vairs nav datu apstrādes pamats. Citiem vārdiem sakot, apstākļi, kādos pārzinis var atsaukties uz šo juridisko pamatu, ir šaurāki nekā agrāk.

Oficiālās pilnvaras vai sabiedrisks uzdevums parasti būtu jāpiešķir normatīvajos aktos vai citos tiesību aktos. DG29 atzinis, ka pēc VDAR šis juridiskais pamats ir jāinterpretē tā, lai publiskajām iestādēm ļautu būt elastīgākām, kas nepieciešams, lai nodrošinātu to pienācīgu pārvaldību un funkcionēšanu. Tādējādi šis noteikums pieļauj datu apstrādi ļoti dažādos gadījumos, kuriem citādi varētu piemērot likumīgu interešu pamatu[24].

Visbeidzot, jāatzīmē, ka datu subjektiem ir tiesības iebilst pret apstrādi, pamatojoties uz šo juridisko pamatu. Pārzinim ir pienākums nepieciešamības gadījumā pierādīt, ka viņam ir pārliecinošs likumīgs pamats personas datu apstrādei[25].

2.5.2. Piemērojamība vietējo pašvaldību darbības kontekstā

Kopā ar juridisko pienākumu, kas minēts VDAR 6.panta 1. punkta c) apakšpunktā, uzdevumam, kas veikts sabiedrības interesēs vai īstenojot oficiālās pilnvaras, būtu jābūt vienam no svarīgākajiem juridiskajiem pamatiem pašvaldību darbā. DG29 sniegtie piemēri par šī pamata piemērošanu ietver:

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

- nodokļu administrācija, kas apkopo un apstrādā personas nodokļu deklarāciju, lai noteiktu un pārbaudītu maksājamā nodokļa summu - pēc analoģijas šo pamatu varētu izmantot arī pašvaldības, kas administrē vietējos nodokļus;
- pašvaldības iestāde, kurai uzticēts uzdevums veikt bibliotēkas pakalpojumus, vadīt skolu vai vietējo peldbaseinu.

2.6. Leģitīmās (likumiskās) intereses

2.6.1. Nozīme un tiesiskās prasības

Juridiskais pamats "leģitīmās intereses" ietver divus elementus:

(i) Datu pārziņa vai trešās personas leģitīmās intereses:

a. Jēdzienu "intereses" DG29 ir definējusi kā pārziņa plašāku ieinteresētību apstrādē vai labumu, ko pārzinis (vai, iespējams, sabiedrība) gūst no datu apstrādes[26]. Intereses varētu dod labumu sabiedrībai kopumā, bet tās varētu būt noderīgas arī tikai attiecīgajam pārzinim vai trešajai pusei;

b. Jēdziens "leģitimitāte" būtībā ir saistīts ar likumu ievērošanu - gan datu aizsardzības likumiem, gan likumiem, kas piemērojami pārziņa attiecīgajai darbībai. Citiem vārdiem sakot, jebkuri nelikumīgi mērķi, ko īsteno pārzinis vai trešā puse, atņem tiesības piemērot šo juridisko pamatu. DG29 ir sniegusi nepilnīgu sarakstu ar visizplatītākajiem scenārijiem, kuros varētu piemērot leģitīmās intereses saskaņā ar vairs spēkā neesošo Direktīvu 95/46. Šīs jomas ir atšķirīgas un sniedzas no reklāmas jeb uzmanības iegūšanas mērķiem (piemēram, tiešais mārketings, reklamējošas vai nepieprasītas nekomerciālas ziņas, tostarp politiskās kampaņas vai labdarības līdzekļu piesaistīšana) līdz sabiedrībai labvēlīgām aktivitātēm (piemēram, pārkāpumu ziņošanas shēmas, tiesību uz vārda brīvību un informāciju izmantošana vai krāpšanas, pakalpojumu ļaunprātīgas izmantošanas vai naudas atmazgāšanas novēršana).

(ii) Datu pārziņa vai trešās personas leģitīmajām interesēm vajadzētu būt samērotām ar datu subjekta interesēm, pamattiesībām un brīvībām = līdzsvarošanas pārbaude jāpiemēro katrā atsevišķā gadījumā. Šī prasība pēc būtības ir saistīta ar proporcionalitātes principu. Lai gan pārzinim vai trešajai pusei var būt leģitīmas intereses veikt datu apstrādi, tas varētu būt nesamērīgi (piemēram, attiecīgā apstrāde varētu būt pārāk mulsinoša, pārāk plaša, bez pienācīgiem ierobežojumiem un drošības pasākumiem utt.), un šādā scenārijā apstrāde nebūtu attaisnojama kā likumīga. DG29 ir norādījusi galvenos faktorus, kas jāņem vērā, lai veiktu līdzsvarošanas pārbaudi:

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

a. pārziņa likumīgo interešu novērtēšana;
b. ietekme uz datu subjektiem;
c. pagaidu līdzsvars un
d. pārziņa īstenoti papildu drošības pasākumi, lai novērstu nepamatotu ietekmi uz datu subjektiem[27].

2.6.2. Piemērojamība vietējo pašvaldību darbības kontekstā

VDAR ievērojami ierobežo leģitīmo interešu pamata piemērojamību publisko iestāžu darbības kontekstā. VDAR skaidri nosaka, ka šo juridisko pamatu nepiemēro apstrādei, ko publiskās iestādes veic, pildot savus uzdevumus. Šīs normas loģiskais pamatojums ir tāds, ka publiskām iestādēm jābūt ar likumu pilnvarotām veikt savus uzdevumus.

Tādēļ pašvaldībām, kuras pamatojas uz leģitīmajām interesēm, veicot savus uzdevumus, ieteicams pārdomāt, kādu citu juridisko pamatu personas datu apstrādei tās varētu piemērot (piemēram, uzdevums, kas tiek veikts sabiedrības interesēs vai īstenojot oficiālās pilnvaras).

Tomēr leģitīmās intereses pašvaldības joprojām varētu piemērot kā derīgu juridisku pamatu saviem iekšējiem procesiem - piemēram, darbībās saistītās ar savu personālu.

3. SECINĀJUMI UN PRAKTISKIE PADOMI

Spēja noteikt, kāds juridiskais pamats piemērojams, attiecīgajai datu apstrādes darbībai ir būtiska katram datu pārzinim, lai nodrošinātu datu apstrādes likumību. Turklāt informācija par to, kurš juridiskais pamats attiecas uz konkrēto apstrādes mērķi, ir viens no caurspīdīguma principa galvenajiem elementiem, jo tas ir skaidri iekļauts informācijā, kas pārzinim jāsniedz katram datu subjektam (VDAR 13. un 14.pants). Tādēļ gan publiskajiem, gan privātajiem datu pārziņiem vajadzētu būt labi informētiem par katra juridiskā pamata, kas minēti VDAR 6.pantā, nozīmi. Regula neparedz jaunus datu apstrādes juridiskos pamatus, bet drīzāk groza prasības un nosacījumus dažu esošo pamatu piemērošanai (piemēram, piekrišanai, leģitīmajām interesēm). Jebkurā gadījumā spēja noteikt pareizu juridisko pamatu ir pirmais solis, lai nodrošinātu VDAR atbilstību organizācijā. Doktrīnā norādīts, ka piesardzīgam datu pārzinim būtu jāveic nepieciešamie pasākumi, lai nodrošinātu, ka gadījumos, kad uzraudzības iestādes pieprasa pierādījumus, datu pārzinim būtu iespēja norādīt, uz kādiem kritērijiem personas datu apstrādē viņš balstās un nodrošina pienācīgu datu subjektu informēšanu[28].

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

4. ĀRĒJIE AVOTI UN TĪMEKĻA VIETNES

Grāmatas

- **Voigt, P., von dem Bussche, A.**, The EU General Data Protection Regulation (GDPR) – A Practical Guide, Springer International Publishing (2017);
- **Boardman, R., Mullock, J., Mole, A.** Bird & Bird Guide to General Data Protection Regulation (2016);
- **EU** General Data Protection Regulation (GDPR). An Implementation and Compliance Guide, IT Governance Publishing, Cambridgeshire (2016);
- **European** Data Protection. Law and Practice, Executive Editor: Edurado Ustaran, CIPP/E, Partner, Hogan Lovells, IAPP (2018)

29.panta darba grupas dokumenti

- WG29, Guidelines on Consent under Regulation 2016/679, WP 259;
- Atzinums 06/2014 par personas datu apstrādātāja likumīgo interešu jēdzienu saskaņā ar Direktīvas 95/46/EK 7. pantu, WP 217;

Tīmekļa saites

- http://europa.eu/rapid/press-release_IP-18-386_en.htm
- https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en
- https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/grounds-processing/when-can-personal-data-be-processed_en
- https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/grounds-processing/what-does-grounds-legitimate-interest-mean_en
- https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/grounds-processing/when-consent-valid_en
- https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/grounds-processing/does-consent-given-25-may-2018-continue-be-valid-once-gdpr-starts-apply-25-may-2018_en
- https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/grounds-processing/what-if-somebody-withdraws-their-consent_en

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

- https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/grounds-processing/what-if-somebody-withdraws-their-consent_en

5. ATSAUCES

[1] WP29, Guidelines on Consent under Regulation 2016/679, WP 259, p. 6.
[2] WP29, Guidelines on Consent under Regulation 2016/679, WP 259, p. 11-12.
[3] Vairāk informācijas par profilēšanu pieejams WP29 Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (projekts).
[4] WP29, Guidelines on Consent under Regulation 2016/679, WP 259, p. 13.
[5] EU General Data Protection Regulation (GDPR). An Implementation and Compliance Guide, IT Governance Publishing, Cambridgeshire (2016), p. 189-190.
[6] WP29, Guidelines on Consent under Regulation 2016/679, WP 259, p. 7.
[7] Piemērs dots WP29, Guidelines on Consent under Regulation 2016/679, WP 259, p. 7.
[8] DG29, Atzinums 06/2014 par personas datu apstrādātāja likumīgo interešu jēdzienu saskaņā ar Direktīvas 95/46/EK 7. pantu, WP 217, 16.-17.lpp.
[9] Turpat, 16.lpp.
[10] Voigt, P., von dem Bussche, A., The EU General Data Protection Regulation (GDPR) – A Practical Guide, Springer International Publishing (2017), p. 102.
[11] European Data Protection. Law and Practice, Executive Editor: Edurado Ustaran, CIPP/E, Partner, Hogan Lovells, IAPP (2018), p. 118.
[12] DG29, Atzinums Nr. 06/2014 par personas datu apstrādātāja likumīgo interešu jēdzienu saskaņā ar Direktīvas 95/46/EK 7. pantu, WP 217, 16.lpp.
[13] Turpat, 19.lpp.
[14] Boardman, R., Mullock, J., Mole, A. Bird & Bird Guide to General Data Protection Regulation (2016), p. 10.
[15] DG29 atzinums Nr. 06/2014 par personas datu apstrādātāja likumīgo interešu jēdzienu saskaņā ar Direktīvas 95/46/EK 7. pantu, WP 217, 19.lpp.
[16] Turpat, 19.lpp.
[17] Turpat, 20.lpp.
[18] Turpat, 19.lpp.
[19] Turpat, 20.lpp.
[20] European Data Protection. Law and Practice, Executive Editor: Edurado Ustaran, CIPP/E, Partner, Hogan Lovells, IAPP (2018), p. 119.
[21] DG29 atzinums Nr. 06/2014 par personas datu apstrādātāja likumīgo interešu jēdzienu saskaņā ar Direktīvas 95/46/EK 7. pantu, WP 217, 20-21.lpp.
[22] Turpat, 21.lpp.
[23] Turpat, 21.lpp.
[24] DG29 atzinums Nr. 06/2014 par personas datu apstrādātāja likumīgo interešu jēdzienu saskaņā ar Direktīvas 95/46/EK 7. pantu, WP 217, 23.lpp.
[25] European Data Protection. Law and Practice, Executive Editor: Edurado Ustaran, CIPP/E, Partner, Hogan Lovells, IAPP (2018), p. 119.
[26] DG29 atzinums Nr. 06/2014 par personas datu apstrādātāja likumīgo interešu jēdzienu saskaņā ar Direktīvas 95/46/EK 7. pantu, WP 217, 24.lpp.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

[27] Turpat, 33.lpp.

[28] European Data Protection. Law and Practice, Executive Editor: Edurado Ustaran, CIPP/E, Partner, Hogan Lovells, IAPP (2018), p. 122.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

ProLegis

Īpašo kategoriju personas datu apstrāde

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

ProLegis

SATURS

1. TIESISKAIS REGULĒJUMS 4
   1.1. ES Pamattiesību harta 4
   1.2. VDAR 4
2. ĪPAŠO KATEGORIJU PERSONAS DATI SASKAŅĀ AR VDAR 9
   2.1. Loģika, kas nosaka atsevišķu kategoriju personas datus kā īpašus 9
   2.2. Īpašo kategoriju personas datu veidi 10
   2.3. Personas dati par sodāmību un pārkāpumiem 11
3. TIESISKIE PAMATI ĪPAŠO KATEGORIJU PERSONAS DATU APSTRĀDEI 12
   3.1. Nepārprotama piekrišana 12
   3.2. Pienākumi vai konkrētas tiesības nodarbinātības, sociālā nodrošinājuma un sociālās aizsardzības tiesību jomā 13
   3.3. Datu subjekta vai citas fiziskas personas vitālās intereses 14
   3.4. Apstrāde, ko veic bezpeļņas struktūra, kas to dara ar politisku, filozofisku, reliģisku vai ar arodbiedrībām saistītu mērķi 14
   3.5. Dati, kurus datu subjekts ir apzināti publiskojis 14
   3.6. Likumīgo prasību celšana, īstenošana vai aizstāvēšana / tiesas pildot savus uzdevumus 15
   3.7. Būtiskas sabiedrības intereses, pamatojoties uz ES vai dalībvalsts tiesību aktiem 15
   3.8. Profilaktiskā vai arodmedicīna, darbinieka darbspējas novērtēšana, medicīniska diagnoze, veselības vai sociālās aprūpes vai ārstēšanas nodrošināšana 15
   3.9. Sabiedrības intereses sabiedrības veselības jomā 16
   3.10. Apstrāde, kas tiek veikta arhivēšanas nolūkos sabiedrības interesēs, zinātniskās vai vēstures pētniecības nolūkos, vai statistikas nolūkos 16
   3.11. Papildu nosacījumi dalībvalstu tiesību aktos 16
4. SECINĀJUMI UN PRAKTISKIE PADOMI 17

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

5. ĀRĒJIE AVOTI UN TĪMEKĻA VIETNES 17
Grāmatas 17
29.panta darba grupas dokumenti 17
Tīmekļa saites 17
6. ATSAUCES 18

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

1. TIESISKAIS REGULĒJUMS

1.1. ES Pamattiesību harta

8.pants

Personas datu aizsardzība

1. Ikvienai personai ir tiesības uz savu personas datu aizsardzību.

*2. Šādi dati ir jāapstrādā godprātīgi, noteiktiem mērķiem un **ar attiecīgās personas piekrišanu vai ar citu likumīgu pamatojumu, kas paredzēts tiesību aktos**. Ikvienam ir pieejas tiesības datiem, kas par viņu savākti, un tiesības ieviest labojumus šajos datos.*

3. Atbilstību šiem noteikumiem kontrolē neatkarīga iestāde.

1.2. VDAR

51.apsvērums

Personas datiem, kas pēc savas būtības ir īpaši sensitīvi saistībā ar pamattiesībām un brīvībām, pienākas īpaša aizsardzība, jo to apstrādes konteksts varētu radīt nopietnu risku pamattiesībām un brīvībām. Minētajiem personas datiem būtu jāaptver personas dati, kuri atklāj rases vai etnisko piederību, turklāt termina "rases piederība" izmatošana šajā regulā nenozīmē, ka Savienība atzīst teorijas, ar kuru palīdzību notiek mēģinājumi noteikt dažādu cilvēku rasu pastāvēšanu. Fotogrāfiju apstrāde nebūtu sistemātiski jāuzskata par īpašu kategoriju personas datu apstrādi, jo uz tām biometrisko datu definīcija attiecas tikai tad, kad tās apstrādās ar konkrētiem tehniskiem līdzekļiem, kas ļauj veikt fiziskas personas unikālu identifikāciju vai autentifikāciju. Šādi personas dati nebūtu jāapstrādā, ja vien apstrāde nav atļauta konkrētos, šajā regulā precizētos gadījumos, ņemot vērā, ka dalībvalstu tiesību aktos var būt paredzēti konkrēti noteikumi par datu aizsardzību, lai pieņemtu šīs regulas noteikumu piemērošanu juridisku pienākumu izpildei vai sabiedrības interesēs veiktu uzdevumu izpildei, vai pārzinim likumīgi piešķirto oficiālo pilnvaru īstenošanai. Papildus konkrētajām prasībām attiecībā uz šādu apstrādi būtu jāpiemēro vispārējie principi un citi šīs regulas noteikumi, jo īpaši attiecībā uz likumīgas apstrādes nosacījumiem. Būtu skaidri jāparedz atkāpes no vispārējā aizlieguma apstrādāt šādu īpašu kategoriju personas datus, cita starpā tad, ja datu subjekts dot nepārprotamu piekrišanu, vai attiecībā uz īpašām vajadzībām, jo īpaši gadījumos, kad apstrādi veic

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

konkrētas apvienības vai nodibinājumi savu leģitīmo darbību ietvaros, kuru nolūks ir atļaut īstenot pamatbrīvības.

52.apsvērums

Atkāpties no aizlieguma apstrādāt īpašu kategoriju personas datus būtu jāatļauj arī tad, ja tas paredzēts Savienības vai dalībvalsts tiesību aktos un ja ir paredzētas atbilstošas garantijas personas datu un citu pamattiesību aizsardzībai, ja to darīt ir sabiedrības interesēs, jo īpaši personas datu apstrāde nodarbinātības tiesību aktu, sociālās aizsardzības tiesību aktu jomā, tostarp attiecībā uz pensijām un veselības drošības, uzraudzības un brīdināšanas nolūkos, lipīgu infekcijas slimību un citu nopietnu veselības apdraudējumu profilaksei vai kontrolei. Šādu atkāpi var veikt ar veselību saistītos nolūkos, tostarp sabiedrības veselības un veselības aprūpes pakalpojumu pārvaldības nolūkos, jo īpaši, lai nodrošinātu pabalstu un veselības apdrošināšanas sistēmas pakalpojumu pieprasīšanai izmantoto procedūru kvalitāti un izmaksu lietderību vai lai veiktu arhivēšanu sabiedrības interesēs, zinātniskās vai vēstures pētniecības nolūkos vai statistikas nolūkos. Atkāpei būtu jāpieļauj arī tādu personas datu apstrāde, kas vajadzīgi, lai celtu, īstenotu vai aizstāvētu likumīgas prasības vai nu tiesas procesā, vai administratīvā vai ārpustiesas procedūrā.

53.apsvērums

Īpašu kategoriju personas datus, kuriem pienākas augstāka aizsardzība, būtu jāapstrādā ar veselību saistītos nolūkos tikai tad, ja minētie nolūki jāsasniedz fizisku personu un visas sabiedrības labā, jo īpaši saistībā ar veselības vai sociālās aprūpes pakalpojumu un sistēmu pārvaldību, tostarp šādu datu apstrādi, ko kvalitātes kontroles nolūkos veic pārvaldības un centrālās valsts veselības iestādes, informāciju par pārvaldību un veselības vai sociālās aprūpes sistēmas vispārēju valsts mēroga un vietēju pārraudzību, un lai nodrošinātu veselības vai sociālās aprūpes un pārrobežu veselības aprūpes nepārtrauktību vai veselības drošību, pārraudzības vai brīdināšanas nolūkos vai arhivēšanas nolūkos sabiedrības interesēs, zinātniskās vai vēstures pētniecības nolūkos vai statistikas nolūkos, pamatojoties uz Savienības vai dalībvalsts tiesību aktiem, kam jāatbilst sabiedrības interešu mērķim, kā arī pētījumiem, kurus sabiedrības veselības jomā veic sabiedrības interesēs. Tāpēc šai regulai būtu jānodrošina saskaņoti nosacījumi īpašu kategoriju personas veselības datu apstrādei attiecībā uz konkrētām vajadzībām, jo īpaši gadījumos, kad šādu datu apstrādi konkrētos ar veselību saistītos nolūkos veic personas, uz kurām attiecas juridiskais pienākums ievērot dienesta noslēpumu. Savienības vai dalībvalsts tiesību aktiem būtu jāparedz konkrēti un atbilstoši pasākumi, lai aizsargātu fizisku personu pamattiesības un personas datus. Būtu jāļauj dalībvalstīm saglabāt vai

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

ieviest papildu nosacījumus, tostarp ierobežojumus, attiecībā uz ģenētisko datu, biometrisko datu vai veselības datu apstrādi. Tomēr tam nevajadzētu kavēt personas datu brīvo plūsmu Savienībā gadījumos, kad minētos nosacījumus piemēro šādu datu pārrobežu apstrādei.

54.apsvērums

Īpašu kategoriju personas datu apstrāde bez datu subjekta piekrišanas var būt nepieciešama sabiedrības interešu dēļ sabiedrības veselības jomās. Uz šādu apstrādi būtu jāattiecas atbilstošiem un konkrētiem pasākumiem fizisku personu tiesību un brīvību aizsardzībai. Minētajā kontekstā "sabiedrības veselība" būtu jāinterpretē saskaņā ar definīciju Eiropas Parlamenta un Padomes Regulā (EK) Nr. 1338/2008, proti, kā visi elementi, kas saistīti ar veselību, proti, veselības stāvoklis, tostarp saslimstība un invaliditāte, faktori, kas ietekmē veselības stāvokli, veselības aprūpes vajadzības, veselības aprūpei piešķirtie resursi, veselības aprūpes nodrošināšana un vispārēja piekļuve tai, kā arī veselības aprūpes izdevumi un finansējums, un nāves cēloņi. Šādai veselības datu apstrādei sabiedrības interešu vārdā nebūtu jānoved pie tā, ka trešās personas, piemēram, darba devēji vai apdrošināšanas sabiedrības un kredītiestādes, apstrādā personas datus citos nolūkos.

55. apsvērums

Turklāt oficiālo iestāžu veiktā oficiāli atzītu reliģisku apvienību personu datu apstrāde, lai sasniegtu konstitucionālajās tiesībās vai starptautiskajās publiskajās tiesībās paredzētus mērķus, tiek veikta, pamatojoties uz sabiedrības interesēm.

56. apsvērums

Ja dalībvalstī vēlēšanu pasākumu laikā demokrātiskās sistēmas darbība prasa, lai politiskās partijas vāktu personas datus par cilvēku politiskajiem uzskatiem, šādu datu apstrādi var pieļaut sabiedrības interešu dēļ, ar noteikumu, ka ir noteikti atbilstoši aizsardzības pasākumi.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

4.pants

Definīcijas

Šajā regulā:

[…]

*13) **“ģenētiskie dati”** ir personas dati, kas attiecas uz fiziskas personas pārmantotajām vai iegūtajām ģenētiskajām pazīmēm, sniedz unikālu informāciju par minētās fiziskās personas fizioloģiju vai veselību un kas izriet jo īpaši no attiecīgās fiziskās personas bioloģiskā parauga analīzes;*

*14) **“biometriskie dati”** ir personas dati pēc specifiskas tehniskas apstrādes, kuri attiecas uz fiziskas personas fiziskajām, fizioloģiskajām vai uzvedības pazīmēm, kas ļauj veikt vai apstiprina minētās fiziskās personas unikālu identifikāciju, piemēram, sejas attēli vai daktiloskopijas dati;*

*15) **“veselības dati”** ir personas dati, kas saistīti ar fiziskas personas fizisko vai garīgo veselību, tostarp veselības aprūpes pakalpojumu sniegšanu, un kas atspoguļo informāciju par tās veselības stāvokli;*

9.pants

Īpašu kategoriju personas datu apstrāde

*1. **Ir aizliegta tādu personas datu apstrāde, kas atklāj rases vai etnisko piederību, politiskos uzskatus, reliģisko vai filozofisko pārliecību vai dalību arodbiedrībās, un ģenētisko datu, biometrisko datu, lai veiktu fiziskas personas unikālu identifikāciju, veselības datu vai datu par fiziskas personas dzimumdzīvi vai seksuālo orientāciju apstrāde.***

*2. **Šā panta 1. punktu nepiemēro**, ja ir piemērojams kāds no šādiem pamatojumiem:*

a) datu subjekts ir devis nepārprotamu piekrišanu šo personas datu apstrādei vienam vai vairākiem konkrētiem nolūkiem, izņemot, ja Savienības vai dalībvalsts tiesību akti paredz, ka 1. punktā minēto aizliegumu datu subjekts nevar atcelt;

b) apstrāde ir vajadzīga, lai realizētu pārziņa pienākumus un īstenotu pārziņa vai datu subjekta konkrētas tiesības nodarbinātības, sociālā nodrošinājuma un sociālās aizsardzības tiesību jomā, ciktāl to pieļauj Savienības vai dalībvalsts tiesību akti vai

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

koplīgums atbilstīgi dalībvalsts tiesību aktiem, paredzot piemērotas garantijas datu subjekta pamattiesībām un interesēm;

c) apstrāde ir vajadzīga, lai aizsargātu datu subjekta vai citas fiziskas personas vitālas intereses, ja datu subjekts ir fiziski vai tiesiski nespējīgs dot savu piekrišanu;

d) veicot leģitīmas darbības un nodrošinot atbilstošas garantijas, apstrādi veic fonds, apvienība vai jebkura cita bezpeļņas struktūra, kas to dara ar politisku, filozofisku, reliģisku vai ar arodbiedrībām saistītu mērķi un ar nosacījumu, ka apstrāde attiecas tikai uz šīs struktūras locekļiem vai bijušajiem locekļiem, vai personām, kas ar šo struktūru uztur regulārus sakarus saistībā ar tās nolūkiem, un ka bez datu subjekta piekrišanas personas datus neizpauž ārpus minētās struktūras;

e) apstrāde attiecas uz personas datiem, kurus datu subjekts apzināti ir publiskojis;

f) apstrāde ir vajadzīga, lai celtu, īstenotu vai aizstāvētu likumīgas prasības, vai ikreiz, kad tiesas pilda savus uzdevumus;

g) apstrāde ir vajadzīga būtisku sabiedrības interešu dēļ, pamatojoties uz Savienības vai dalībvalsts tiesību aktiem, kas ir samērīgas izvirzītajam mērķim, ievēro tiesību uz datu aizsardzību būtību un paredz piemērotus un konkrētus pasākumus datu subjekta pamattiesību un interešu aizsardzībai;

h) apstrāde ir vajadzīga profilaktiskās vai arodmedicīnas nolūkos, darbinieka darbspējas novērtēšanai, medicīniskas diagnozes, veselības vai sociālās aprūpes vai ārstēšanas vai veselības vai sociālās aprūpes sistēmu un pakalpojumu pārvaldības nodrošināšanas nolūkos, pamatojoties uz Savienības vai dalībvalsts tiesību aktiem vai saskaņā ar līgumu ar veselības darba profesionāli un ievērojot 3. punktā minētos nosacījumus un garantijas;

i) apstrāde ir vajadzīga sabiedrības interešu dēļ sabiedrības veselības jomā, piemēram, aizsardzībai pret nopietniem pārrobežu draudiem veselībai vai augstu kvalitātes un drošības standartu nodrošināšanai, cita starpā zālēm vai medicīniskām ierīcēm, pamatojoties uz Savienības vai dalībvalsts tiesību aktiem, kas paredz atbilstošus un konkrētus pasākumus datu subjekta tiesību un brīvību, jo īpaši dienesta noslēpuma, aizsardzībai;

j) apstrāde ir vajadzīga arhivēšanas nolūkos sabiedrības interesēs, zinātniskās vai vēstures pētniecības nolūkos, vai statistikas nolūkos saskaņā ar 89. panta 1. punktu, pamatojoties uz Savienības vai dalībvalsts tiesību aktiem, kas ir samērīgi izvirzītajam mērķim, ievēro tiesību uz datu aizsardzību būtību un paredz piemērotus un konkrētus pasākumus datu subjekta pamattiesību un interešu aizsardzībai.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

3. Šā panta 1. punktā minētos personas datus var apstrādāt 2. punkta h) apakšpunktā minētajos nolūkos, ja šos datus apstrādā profesionālis, uz kuru saskaņā ar Savienības vai dalībvalsts tiesību aktiem vai valsts kompetento iestāžu ieviestiem noteikumiem attiecas dienesta noslēpuma ievērošanas pienākums, vai ja tos apstrādā šāda profesionāļa atbildībā; vai cita persona, uz kuru arī attiecas pienākums ievērot dienesta noslēpumu saskaņā ar Savienības vai dalībvalsts tiesību aktiem vai valsts kompetento iestāžu ieviestiem noteikumiem.

4. Dalībvalstis var saglabāt vai ieviest papildu nosacījumus, tostarp ierobežojumus, attiecībā uz ģenētisko datu, biometrisko datu vai veselības datu apstrādi.

10.pants

Personas datu par sodāmību un pārkāpumiem apstrāde

***Personas datu apstrādi par sodāmību un pārkāpumiem vai ar tiem saistītiem drošības pasākumiem**, pamatojoties uz 6. panta 1. punktu, veic **tikai oficiālas iestādes kontrolē vai tad, ja apstrādi atļauj Savienības vai dalībvalsts tiesību akti**, paredzot atbilstošas garantijas datu subjektu tiesībām un brīvībām. Jebkādu visaptverošu sodāmības reģistru uzglabā tikai oficiālas iestādes kontrolē.*

2. ĪPAŠO KATEGORIJU PERSONAS DATI SASKAŅĀ AR VDAR

2.1. Loģika, kas nosaka atsevišķu kategoriju personas datus kā īpašus

Jau sagatavojot pirmo ES tiesību aktu, kas tika veltīts personas datu aizsardzībai - Direktīvu 95/46 - Eiropas Komisija uzsvēra, ka dažu kategoriju personas datu apstrāde varētu radīt lielāku risku Eiropas pilsoņu pamattiesībām un brīvībām[1]. Tādējādi tika noteikts vispārējs aizliegums apstrādāt šādas "riskantas" personas datu kategorijas. Tie tika saukti par " īpašu kategoriju personas datiem", taču praksē saukti arī par "sensitīviem datiem" to sensitīvā rakstura dēļ, kas var ietekmēt personas privāto telpu[2]. Šos datus var apstrādāt tikai ārkārtas apstākļos, kas precīzi uzskaitīti dalībvalstu datu aizsardzības tiesību aktos.

VDAR turpina šo pieeju, bet paplašina īpašo kategoriju personas datu loku un paredz dažus jaunus izņēmumus (tiesisko pamatojumu), kas pārzinim dod tiesības apstrādāt šādus datus.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

Jāatzīmē, ka dažāda veida dati dažādi ietekmē personas. Tie dati, kuri definēti kā sensitīvi, pamatojas uz objektīvu un nevis uz subjektīvu principu. Citiem vārdiem sakot, kāds varētu uzskatīt, ka dati, kas saistīti ar viņu finansiālo stāvokli, disciplināro sodu vēsturi vai personas identifikācijas numuru/sociālās apdrošināšanas numuru, ir sensitīvi. Tomēr, ja Eiropas likumdevējs šādus datus neatzīst kā sensitīvus, uz tiem neattiecas īpašais datu apstrādes režīms neatkarīgi no subjektīvā viedokļa par to sensitīvo raksturu.

Doktrīnā norādīts, ka izvēli par to, kuru kategoriju personas datus definēt kā īpašus, būtiski ietekmēja diskriminācijas novēršanas tiesību akti, kas izskaidro, kāpēc tādi dati kā sociālās apdrošināšanas numuri un kredītkaršu dati (kas, ļaunprātīgi izmantoti varētu radīt nopietnus kaitējumus personām) nav definēti kā sensitīvi[3].

2.2. Īpašo kategoriju personas datu veidi

Saskaņā ar VDAR 9.panta 1.punktu, sekojoša veida personas dati ir īpašas kategorijas (sensitīvi dati):

- **Personas dati, kas atklāj rasi vai etnisko piederību** = šīs kategorijas personas dati ir definēti kā sensitīvi, jo tie saistīti ar lielu diskriminācijas risku. Tiesiskajā doktrīnā ir minēti piemēri par to, kādi dati var ietilpt šajā kategorijā: personas vārds un uzvārds, viņa dzimšanas vieta, viņa dzimtā valoda vai viņa vecāku vārdi, kuri apvienojumā ļauj secināt viņa izcelsmi[4];
- **Politiskie uzskati** = šiem datiem nepieciešama īpaša aizsardzība, jo tie ir saistīti ar pilsoņu tiesībām veidot viedokļus par politiku, kā arī piedalīties (aktīvi kā politiķi un/vai pasīvi kā vēlētāji un pilsoniskās sabiedrības pārstāvji) valsts politiskajā dzīvē. Šādu datu piemēri ietver informāciju par piederību politiskajai partijai, informāciju par pievienošanos jebkādai petīcijai, piedalīšanos demonstrācijās, politisko atkalapvienošanos vai līdzīgiem pasākumiem, informāciju par kādas politiskās idejas atbalstu vai tās noraidīšanu[5];
- **Reliģiskā vai filozofiskie pārliecība** = šī datu kategorija ir cieši saistīta ar sirdsapziņas brīvību, t.i., brīvību izlemt, vai ticēt pārpasaulīgajiem spēkiem, kas nosaka mūsu ikdienas dzīvi un vai to paust citiem vai ne. Cilvēces vēsture ir pilna ar piemēriem, kad vardarbība notikusi, pamatojoties uz reliģiskajām atšķirībām, tādēļ šādi dati arī būtu īpaši jāaizsargā saskaņā ar datu aizsardzības tiesību aktiem;
- **Dalība arodbiedrībās** = informācija par šādu dalību ir sensitīva, jo tā rada diskriminējošu attieksmi darba tiesību jomā. Eiropas pilsoņiem ir brīvība slēgt darba koplīgumus un kolektīvi rīkoties, tāpēc pret viņiem nevajadzētu izturēties nevienlīdzīgi, pamatojoties uz viņu arodbiedrību piederību[6];

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

- **Ģenētiskie dati** = jauna kategorija, ko VDAR ieviesusi kā sensitīvus datus. VDAR to definē kā "dati, kas attiecas uz fiziskas personas pārmantotajām vai iegūtajām ģenētiskajām pazīmēm, sniedz unikālu informāciju par minētās fiziskās personas fizioloģiju vai veselību un kas izriet jo īpaši no attiecīgās fiziskās personas bioloģiskā parauga analīzes". Dažas dalībvalstis jau ir piešķīrušas šāda veida datiem sensitīvu datu statusu[7], bet VDAR pirmo reizi to ievieš ES līmenī. Ģenētiskie dati ir jāaizsargā, jo šāda veida dati attiecas ne tikai uz attiecīgo datu subjektu, bet arī potenciāli var ietekmēt nenoteiktu personu loku, kas ir daļa no šī subjekta radiniekiem (tostarp mirušo personu dati, bērnu dati utt.). Turklāt šādu datu detalizēta analīze varētu atklāt citu konfidenciālu informāciju, piemēram, datus par psiholoģisko vai veselības stāvokli (piemēram, noslieces uz slimībām, psihiskajiem traucējumiem utt.);
- **Biometriskie dati, lai veiktu fiziskas personas unikālu identifikāciju** = šāda veida datiem nepieciešama aizsardzība, jo tie ļauj pārziņiem nepārprotami identificēt konkrētu fizisku personu, pamatojoties uz to fiziskajām vai uzvedības īpašībām: pirkstu nospiedumi, sejas atpazīšana, varavīksnene, tīklene, asinsvadu topoloģija, DNS, runa, paraksts, taustiņu spiešana utt.). Tā kā šāda veida datu apstrāde kļūst arvien izplatītāka, ieviešot dažādus tehnoloģiskus risinājumus (piemēram, telpu piekļuves kontroles sistēmas, identifikācijas sistēmas tālvadības ierīcēs, piemēram, mobilajos tālruņos, planšetdatoros utt.), šāda apstrāde jāveic stingrāk un kontrolētāk, un šie faktori pamato šo datu iekļaušanu "sensitīvo" datu sarakstā saskaņā ar VDAR. Pretēji praksei, kas izveidota dažās dalībvalstīs, fotogrāfiju apstrāde netiks automātiski uzskatīta par sensitīvu apstrādi. Fotogrāfijas tiks uzskatītas par sensitīviem datiem tikai tad, ja tās ļaus biometrisku personas unikālu identifikāciju vai autentifikāciju (piem., elektroniskajā pasē vai cita veida identifikācijas dokumentā)[8];
- **Dati par veselību vai dati par fiziskas personas dzimumdzīvi vai seksuālo orientāciju** = šādi dati ir ļoti sensitīvi, jo tie skar cilvēka dzīves visintīmākos aspektus. Turklāt informācija par dzimumdzīvi un seksuālo orientāciju var radīt diskriminācijas, manipulācijas u.c. riskus. Teorētiski noteikts, ka šie dati ietver arī personas partnera(-u) precīzu identitāti[9].

2.3. Personas dati par sodāmību un pārkāpumiem

Personas dati par sodāmību un pārkāpumiem vai ar tiem saistīti drošības pasākumi **nav** noteikti par īpašu kategoriju personas datiem. Tomēr dažu dalībvalstu tiesību akti tos uzskata par sensitīviem[10]. Šāda veida informācija var radīt nevienlīdzīgas attieksmes risku (piemēram, nodarbinātības jomā), tāpēc arī uz šiem datiem attiecas īpaši apstrādes noteikumi. Attiecībā uz datiem par sodāmību un pārkāpumiem VDAR neievieš būtiskas

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

izmaiņas salīdzinājumā ar vairs spēkā neesošo Direktīvu 95/46. Tajā pašā laikā, ņemot vērā faktu, ka direktīvas noteikumi dalībvalstīs tika transponēti dažādi, VDAR ieviesīs vispārēju pieeju attiecībā uz šādiem datiem ES līmenī. Saskaņā ar VDAR 10.pantu, šos datus var apstrādāt, pamatojoties uz vienu no tiesiskajiem pamatiem 6.pantā, ja tiek izpildīts viens no diviem **alternatīviem** papildu nosacījumiem:

1) apstrāde tiek veikta oficiālas iestādes kontrolē vai
2) apstrādi atļauj ES vai dalībvalsts tiesību akti, paredzot atbilstošas garantijas datu subjektu tiesībām un brīvībām.

Pastāv neskaidrības saistībā ar šo nosacījumu, jo nav skaidrs, kā šīs divas papildu prasības, piemērojamas kopā ar 6.pantu. Konservatīvā interpretācija ir tāda, ka privātas vai komerciālas organizācijas nevar apstrādāt šādus datus, citiem vārdiem sakot, "regula neatļauj šādu datu privātu vai komerciālu apstrādi"[11]. Cita interpretācija ir tāda, ka šāda veida datus var apstrādāt pamatojoties uz jebkuru no iespējamajiem tiesiskajiem pamatiem ar nosacījumu, ka tiek izpildīti papildu nosacījumi (oficiālas iestādes kontrolē vai, ja to pieļauj piemērojamie tiesību akti). Doktrīnā norādīts, ka šis noteikums, iespējams, novedīs pie pastāvīgām atšķirībām valstīs[12]. Lai arī vietējās pašvaldības darbojas kā publiskas iestādes un teorētiski varētu izpildīt pirmo apstrādes papildu prasību (oficiālas iestādes kontrolē), joprojām būtu ieteicams rūpīgi pārbaudīt savus nacionālos tiesību aktus, kuri norāda, kādos gadījumos šāda veida dati varētu tikt apstrādāti (jo īpaši saistībā ar darbībām, kas skar cilvēkresursus un sodāmības datu apkopošanu, jo attiecīgā pašvaldība drīzāk darbosies kā darba devējs šādā kontekstā, nevis kā publiskas varas turētājs, tāpēc pirmā papildu nosacījuma piemērojamība ir apšaubāma).

3. TIESISKIE PAMATI ĪPAŠO KATEGORIJU PERSONAS DATU APSTRĀDEI

Vispārējs aizliegums apstrādāt īpašo kategoriju personas datus netiek piemērots, ja tiek izpildīts viens no zemāk minētajiem **alternatīvajiem** nosacījumiem:

3.1. Nepārprotama piekrišana

Jebkurā gadījumā uz īpašo kategoriju personas datu apstrādi attiecas prasības, kas jāizpilda saskaņā ar VDAR, lai iegūtu derīgu piekrišanu (brīvi sniegtu, konkrētu, informētu, viennozīmīgu). Jēdziens "nepārprotams" nav definēts VDAR. 29. panta darba grupa (DG29) norādījusi, ka ir nepieciešama nepārprotama piekrišana gadījumos, kad rodas nopietns datu aizsardzības risks, un ir piemērota augsta līmeņa personas datu individuāla kontrole[13].

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

Jēdziens "nepārprotams" attiecas uz veidu, kādā datu subjekts izsaka piekrišanu - datu subjektam jāsniedz skaidrs piekrišanas apliecinājums. Viens no veidiem, kā dot piekrišanu, ir to skaidri apstiprināt rakstiski[14]. Tiešsaistē var izmantot dažādus risinājumus, aizpildot elektronisko veidlapu, nosūtot e-pastu, augšupielādējot skenētu dokumentu ar datu subjekta parakstu vai izmantojot elektronisko parakstu. Piemēroti varētu būt jebkādi citi līdzekļi, kas ļautu datu pārzinim pierādīt augsto slieksni, kādā piekrišana sniedzama.

Ņemot vērā pilnvaru nesabalansētību starp datu subjektiem un publiskām iestādēm, pašvaldībām nav ieteicams pamatoties galvenokārt uz nepārprotamu piekrišanu īpašu kategoriju personas datu apstrādē (tostarp attiecībās ar iedzīvotājiem un darbiniekiem).

3.2. Pienākumi vai konkrētas tiesības nodarbinātības, sociālā nodrošinājuma un sociālās aizsardzības tiesību jomā

Šis nosacījums īpaši attiecas uz pašvaldībām, vadot savus iekšējos personāla procesus. Īpašo kategoriju personas datu apstrāde varētu būt nepieciešama visos darba attiecību posmos - sākumā (jauna personāla pieņemšanas procesā), izpildes un izmaiņu posmā, un galu galā pie darba attiecību izbeigšanas.

Piemēri, kuros šāda apstrāde varētu būt nepieciešama, ietver darbnespējas un grūtniecības un dzemdību atvaļinājumu administrēšanu; darbinieku pāriešanu piemērotākā amatā veselības apsvērumu dēļ pēc veselības aprūpes iestāžu pieprasījuma; ievērojot obligātos noteikumus, kas paredz noteiktu kategoriju darbinieku aizsardzību, ja tiek pārtrauktas darba attiecības utt.

VDAR ieviestās vispārīgās prasības šī pamata lietojumiem ir šādas:

1) Apstrādei jābūt nepieciešamai, lai izpildītu datu pārziņa pienākumus vai konkrētas datu subjekta tiesības;
2) Šie pienākumi vai tiesības atrunātas ES vai dalībvalstu tiesību aktos vai koplīgumā;
3) nodrošinātas piemērotas garantijas datu subjekta pamattiesībām un interesēm.

Lai piemērotu šo juridisko pamatu, ir jāievēro noteikti dalībvalsts nacionālie tiesību akti, kur pašvaldības darbojas kā darba devējs. Tā kā nodarbinātības tiesības ir viena no jomām, kur VDAR pilnvaro dalībvalstis pieņemt papildu tiesību aktus attiecībā uz personas datu aizsardzību (88.pants), pašvaldībām, izmantojot šo pamatu, piemērota vietēja mēroga pieeja.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

3.3. Datu subjekta vai citas fiziskas personas vitālās intereses

Līdzīgi juridiskajam pamatam saskaņā ar VDAR 6.panta 1.punkta d) apakšpunktu, šāda situācija attiecas uz apstākļiem, kas saistīti ar dzīvību vai nāvi[15]. Tās varētu būt datu subjekta vai kādas citas personas vitālās intereses. Atšķirīgais salīdzinājumā ar 6.pantu ir tas, ka pārzinim ir pienākums pierādīt papildu nosacījuma esamību, proti, ka "datu subjekts ir fiziski vai juridiski nespējīgs dot savu piekrišanu". Šis formulējums nozīmē, ka pārzinim pirms tam jācenšas iegūt datu subjekta piekrišana[16].

3.4. Apstrāde, ko veic bezpeļņas struktūra, kas to dara ar politisku, filozofisku, reliģisku vai ar arodbiedrībām saistītu mērķi

Iespēja apstrādāt sensitīvus datus saskaņā ar šo juridisko pamatu ir paredzēta konkrētām bezpeļņas organizācijām, piemēram, politiskajām partijām, fondiem, baznīcām, citām filozofisko, reliģisko vai arodbiedrību organizāciju formām. Šādas organizācijas var apstrādāt sensitīvus datus, ja:

a) šie dati attiecas tikai uz šīs struktūras locekļiem vai bijušajiem locekļiem, vai personām, kas ar šo struktūru uztur regulārus sakarus;
b) apstrāde tiek veikta to leģitīmo darbību ietvaros;
c) apstrāde tiek veikta saistībā ar to konkrētiem nolūkiem;
d) nodrošināta datu subjektu pamattiesību aizsardzība atbilstošā līmenī;
e) personas dati netiek izpausti ārpus minētās struktūras bez datu subjekta piekrišanas.

Citas konkrētas prasības jāmeklē nacionālajos tiesību aktos[17].

Šis juridiskais pamats gandrīz praktiski nav piemērojams pašvaldību darbības gaitā.

3.5. Dati, kurus datu subjekts ir apzināti publiskojis

Ja datu subjekts savus personas datus apzināti atklāj plašai sabiedrībai, tad tiek pieņemts, ka datu subjekts ir atteicies no īpašās aizsardzības, kas piešķirta šādai informācijai. Jebkurā gadījumā lēmumam atklāt šādu informāciju jābūt indivīda brīvas izvēles rezultātam[18]. Šādu datu atklāšana var izpausties dažādos veidos - dati no publiski pieejamiem reģistriem, vietnēm, sarakstiem, forumiem vai pat no profila sociālajā tīklā, kas ir pieejams bez lietotāja konta utt.[19] Jebkurā gadījumā fakts, ka šie dati ir apzināti publiskoti neatbrīvo pārzini no pienākuma ievērot citas VDAR prasības - piemēram, ievērot datu aizsardzības principus, ievērot privātumu pēc noklusējuma un integrētu privātumu, veikt attiecīgus pasākumus, lai garantētu datu drošību utt.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

3.6. Likumīgo prasību celšana, īstenošana vai aizstāvēšana / tiesas pildot savus uzdevumus

Atsevišķos gadījumos sensitīvu datu apstrāde var būt nepieciešama, lai celtu, īstenotu vai aizstāvētu likumīgas prasības. Pārzinim ir pienākums pierādīt, ka šāda apstrāde ir nepieciešama, t.i., ka starp apstrādi un nolūkiem pastāv cieša un būtiska saistība[20]. Šādas situācijas varētu ietvert, piemēram, administratīvajā tiesā iesniegtas pārsūdzības par pašvaldību izdotiem aktiem, ja sensitīvu datu apstrāde notika iepriekšējās administratīvās procedūras laikā; darba strīdi, kuros pašvaldībām kā darba devējiem būtu jāņem vērā darbinieku dati par veselības stāvokli utt.

Papildus tam, tiesu darbības ietvaros veiktā apstrāde arī var tikt pamatota ar šādu kategoriju personas datu apstrādi.

3.7. Būtiskas sabiedrības intereses, pamatojoties uz ES vai dalībvalsts tiesību aktiem

Šis VDAR noteikums ļauj dalībvalstīm ieviest savos nacionālajos tiesību aktos īpašu noteikumu, kas ļauj apstrādāt sensitīvus datus, pamatojot šādu apstrādi ar būtiskām sabiedrības interesēm.

Jebkurā gadījumā, lai izpildītu VDAR prasības, dalībvalstīm jānodrošina, ka:

1) apstrāde ir samērīga ar izvirzīto mērķi;
2) tiek ievērota tiesību uz datu aizsardzību būtība;
3) pieņemtie tiesību akti paredz piemērotus un konkrētus pasākumus datu subjekta pamattiesību un interešu aizsardzībai.

Jāskatās, kā šī iespēja tiks izmantota nākotnē. Pašvaldībām ieteicams veikt attiecīgo vietējo tiesību aktu analīzi, lai noteiktu, vai viņi var paļauties uz šādu pamatu.

3.8. Profilaktiskā vai arodmedicīna, darbinieka darbspējas novērtēšana, medicīniska diagnoze, veselības vai sociālās aprūpes vai ārstēšanas nodrošināšana

Aizliegums apstrādāt īpašo kategoriju personas datus neattiecas uz apstrādi, kas tiek veikta medicīniskās vai sociālās aprūpes nolūkos[21]. Šāda apstrāde var notikt dažādās jomās, piemēram, arodmedicīnā, medicīniskajā diagnozē vai pakalpojumu sniegšanā sociālās vai medicīniskās aprūpes jomā. Šāda apstrāde var notikt, pamatojoties uz ES vai dalībvalstu tiesību aktiem vai saskaņā ar līgumu ar veselības aprūpes speciālistu[22]. Papildus tam VDAR 9.panta 3.punkts ļauj sensitīvus datus apstrādāt personai, uz kuru attiecas dienesta noslēpuma ievērošanas pienākums.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

Šis juridiskais pamats attiecas uz ārstiem, medicīnas māsām un citām personām, kas iesaistītas veselības aprūpes pakalpojumu sniegšanā[23].

No praktiskā viedokļa šis noteikums ļautu pašvaldībai kā darba devējam nodrošināt arodmedicīnas pakalpojumus, kā daļu no pienākuma nodrošināt veselībai un drošībai labvēlīgus darba apstākļus.

3.9. Sabiedrības intereses sabiedrības veselības jomā

Saskaņā ar VDAR 54.apsvērumu "sabiedrības veselība" ir jāinterpretē saskaņā ar definīciju Regulā (EK) Nr. 1338/2008, proti, kā visi elementi, kas saistīti ar veselību, proti, veselības stāvoklis, tostarp saslimstība un invaliditāte, faktori, kas ietekmē veselības stāvokli, veselības aprūpes vajadzības, veselības aprūpei piešķirtie resursi, veselības aprūpes nodrošināšana un vispārēja piekļuve tai, kā arī veselības aprūpes izdevumi un finansējums, un nāves cēloņi.

Iemesli, kas varētu attaisnot šī juridiskā pamata piemērošanu, varētu būt aizsardzība pret nopietniem pārrobežu veselības apdraudējumiem vai augstu veselības aprūpes, medicīnas produktu vai medicīnas ierīču kvalitātes un drošības standartu nodrošināšana[24].

Veselības datu apstrāde sabiedrības interešu labad nedrīkst novest pie tā, ka trešās personas (piemēram, darba devēji vai apdrošināšanas un banku uzņēmumi) apstrādā personas datus citiem mērķiem.

3.10. Apstrāde, kas tiek veikta arhivēšanas nolūkos sabiedrības interesēs, zinātniskās vai vēstures pētniecības nolūkos, vai statistikas nolūkos

Šādu mērķu apstrādei jābalstās uz dalībvalstu vai ES tiesību aktiem. VDAR pieprasa, lai tiesību normas, kas atļauj šādu apstrādi būtu: samērīgas ar izvirzītajam mērķim, ievēro tiesību uz datu aizsardzību būtību un paredz piemērotus un konkrētus pasākumus datu subjekta pamattiesību un interešu aizsardzībai. Ieviestajiem aizsardzības pasākumiem jāatbilst attiecīgo personas datu sensitīvajam raksturam[25].

3.11. Papildu nosacījumi dalībvalstu tiesību aktos

VDAR 9.panta 4.punkts atļauj dalībvalstīm ieviest papildu nosacījumus vai ierobežojumus noteiktu īpašo kategoriju personas datu apstrādei, proti: ģenētiskie dati, biometrijas dati vai dati par veselību. Tādējādi turpmāk jāuzrauga vietējie tiesību akti, kas piemērojami pašvaldībās.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

4. SECINĀJUMI UN PRAKTISKIE PADOMI

Pašvaldībām būtu jāapzinās, ka noteiktām personas datu kategorijām nepieciešama īpaša aizsardzība, jo tās būtībā ir saistītas ar cilvēka dzīves visintīmākajiem aspektiem un/vai var radīt diskriminācijas riskus. Parasti šādu datu apstrāde ir aizliegta, ja vien nav papildus nosacījumu (izņēmumi).

Vispraktiskākie aspekti, kas varētu ietekmēt pašvaldību darbības, ir darbinieku veselības datu apstrāde. VDAR ļauj veikt šādu apstrādi, bet tikai tad, ja tas ir nepieciešams pārziņa pienākumu veikšanai (vai datu subjekta tiesībām) saskaņā ar darba tiesībām.

Dati par sodāmību un pārkāpumiem nav īpaša kategorija, bet uz tiem arī attiecas īpašais datu apstrādes režīms saskaņā ar VDAR. Ņemot vērā VDAR, būtu jāpārskata personāla vadības prakses sodāmības datu apkopošanā vai veicot nākamo darbinieku iepriekšējo darbību plašas pārbaudes.

5. ĀRĒJIE AVOTI UN TĪMEKĻA VIETNES

Grāmatas

- **Boardman, R., Mullock, J., Mole, A.** Bird & Bird Guide to General Data Protection Regulation (2016);
- **Ehmann, E., Helfrich, M.** EG Datenschutzrichtlinie: Kurzkommentar, Verlag Dr. Otto Schmidt, Koln, (1999)
- **Voigt, P., von dem Bussche, A.**, The EU General Data Protection Regulation (GDPR) – A Practical Guide, Springer International Publishing (2017);
- **EU** General Data Protection Regulation (GDPR). An Implementation and Compliance Guide, IT Governance Publishing, Cambridgeshire (2016);
- **European** Data Protection. Law and Practice, Executive Editor: Edurado Ustaran, CIPP/E, Partner, Hogan Lovells, IAPP (2018);

29.panta darba grupas dokumenti

- DG29, Vadlīnijas par piekrišanu saskaņā ar Regulu (ES) 2016/679, WP 259;
- DG29, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, WP 217;

Tīmekļa saites

- http://europa.eu/rapid/press-release_IP-18-386_en.htm
- https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

- https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/sensitive-data/what-personal-data-considered-sensitive_en
- https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/sensitive-data/under-what-conditions-can-my-company-organisation-process-sensitive-data_en

6. ATSAUCES

[1] Ehmann, E., Helfrich, M. EG Datenschutzrichtlinie: Kurzkommentar, Verlag Dr. Otto Schmidt, Koln, (1999), p. 130-131.
[2] VDAR skaidri atzīst jēdzienu "sensitīvi dati" - sk., piemēram, 10. apsvērumu.
[3] European Data Protection. Law and Practice, Executive Editor: Edurado Ustaran, CIPP/E, Partner, Hogan Lovells, IAPP (2018), p. 123.
[4] Voigt, P., von dem Bussche, A., The EU General Data Protection Regulation (GDPR) – A Practical Guide, Springer International Publishing (2017), p. 111.
[5] Ibid, p. 111.
[6] Ibid, p. 111.
[7] Bulgarijā šādi dati ir sensitīvi kopš 2005.gada.
[8] Boardman, R., Mullock, J., Mole, A. Bird & Bird Guide to General Data Protection Regulation (2016), p.18.
[9] Voigt, P., von dem Bussche, A., The EU General Data Protection Regulation (GDPR) – A Practical Guide, Springer International Publishing (2017), p. 111.
[10] Boardman, R., Mullock, J., Mole, A. Bird & Bird Guide to General Data Protection Regulation (2016), p. 19.
[11] EU General Data Protection Regulation (GDPR). An Implementation and Compliance Guide, IT Governance Publishing, Cambridgeshire (2016), p. 196.
[12] Boardman, R., Mullock, J., Mole, A. Bird & Bird Guide to General Data Protection Regulation (2016), p. 19.
[13] WP29, Guidelines on Consent under Regulation 2016/679, WP 259, p. 18.
[14] Ibid, p. 18.
[15] Ibid, p. 126.
[16] Ibid, p. 126.
[17] Ibid, p. 126-127.
[18] Voigt, P., von dem Bussche, A., The EU General Data Protection Regulation (GDPR) – A Practical Guide, Springer International Publishing (2017), p. 113.
[19] Ibid, p. 113.
[20] European Data Protection. Law and Practice, Executive Editor: Edurado Ustaran, CIPP/E, Partner, Hogan Lovells, IAPP (2018), p. 127.
[21] Ibid, p. 128.
[22] Ibid, p. 129.
[23] Ibid, p. 129.
[24] Voigt, P., von dem Bussche, A., The EU General Data Protection Regulation (GDPR) – A Practical Guide, Springer International Publishing (2017), p. 114.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

[25] Ibid, p. 115.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

ProLegis

Datu aizsardzības speciālista (DAS) iecelšana, amats un funkcijas

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

ProLegis

Saturs

1. TIESISKAIS REGULĒJUMS 4

VDAR 4

2. DAS IECELŠANA 7

2.1. Obligāta iecelšana saskaņā ar VDAR 7

2.1.1. Publiska iestāde vai struktūra 7

2.1.2. Pārziņa vai apstrādātāja pamatdarbība […], kurai nepieciešama regulāra un sistemātiska datu subjektu novērošana plašā mērogā 7

2.1.3. Pārziņa vai apstrādātāja pamatdarbības ietver īpašo kategoriju datu […] un personas datu par sodāmību un pārkāpumiem apstrādi plašā mērogā 8

2.2. DAS iecelšana citās situācijās 9

2.2.1. Obligātā iecelšana saskaņā ar ES vai dalībvalstu tiesību aktiem 9

2.2.2. Brīvprātīga iecelšana 9

2.3. Līgumiskās attiecības ar DAS 10

2.3.1. Darba līgums 10

2.3.2. Pakalpojuma līgums 10

3. DAS AMATS 10

3.1. Iesaistīšana visos jautājumos, kas saistīti ar personas datu aizsardzību 10

3.2. Nepieciešamo resursu un neatkarības nodrošināšana 11

3.3. Interešu konflikts 12

4. DAS UZDEVUMI 13

4.1. Uzraudzība 13

4.2. Novērtējums par ietekmi uz datu aizsardzību (NIDA) 13

4.3. Kontaktpunkts 13

4.4. Datu uzglabāšana 14

5. SECINĀJUMI UN PRAKTISKIE PADOMI 14

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

6. ĀRĒJIE AVOTI UN TĪMEKĻA VIETNES 15
Grāmatas 15
29.panta darba grupas dokumenti 15
Tīmekļa saites 15
7. ATSAUCES 15

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

1. TIESISKAIS REGULĒJUMS

VDAR

97.apsvērums

Ja datu apstrādi veic publiska iestāde, izņemot tiesas vai neatkarīgas tiesu iestādes, kad tās pilda tiesas funkciju, ja privātajā sektorā apstrādi veic pārzinis, kura pamatdarbības sastāv no apstrādes darbībām, kam nepieciešama regulāra un sistemātiska datu subjektu novērošana plašā mērogā, vai ja datu pārziņa vai apstrādātāja pamatdarbības ietver īpašo kategoriju personas datu un datu par sodāmību un pārkāpumiem apstrādi plašā mērogā, personai ar speciālām zināšanām datu aizsardzības tiesību un prakses jomā būtu jāpalīdz pārzinim vai apstrādātājam uzraudzīt to, kā iekšēji tiek ievērota šī regula. Privātajā sektorā pārziņa pamatdarbības ir saistītas ar tā galvenajām darbībām, un tās nav saistītas ar personas datu apstrādi kā palīgdarbības. Nepieciešamais speciālo zināšanu līmenis būtu jānosaka jo īpaši saskaņā ar veiktajām datu apstrādes darbībām un aizsardzību, kas nepieciešama personas datiem, kurus pārzinis vai apstrādātājs apstrādā. Šādiem datu aizsardzības speciālistiem neatkarīgi no tā, vai pārzinis ir to darba devējs, būtu jāspēj neatkarīgi pildīt savus pienākumus un uzdevumus.

37.pants

Datu aizsardzības speciālista iecelšana

1. Pārzinis un apstrādātājs ieceļ datu aizsardzības speciālistu katrā gadījumā, kad:

(a) apstrādi veic publiska iestāde vai struktūra, izņemot tiesas, tām pildot savus uzdevumus;

(b) pārziņa vai apstrādātāja pamatdarbība sastāv no apstrādes darbībām, kurām to būtības, apmēra un/vai nolūku dēļ nepieciešama regulāra un sistemātiska datu subjektu novērošana plašā mērogā; vai

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

(c) pārziņa vai apstrādātāja pamatdarbības ietver īpašo kategoriju datu saskaņā ar 9. pantu un 10. pantā minēto personas datu par sodāmību un pārkāpumiem apstrādi plašā mērogā.

2. Uzņēmumu grupa var iecelt vienu datu aizsardzības speciālistu ar noteikumu, ka katrs uzņēmums var viegli sazināties ar datu aizsardzības speciālistu.

3. Ja pārzinis vai apstrādātājs ir publiska iestāde vai struktūra, vienu datu aizsardzības speciālistu var iecelt vairākām šādām iestādēm vai struktūrām, ņemot vērā to organizatorisko uzbūvi un lielumu.

4. Gadījumos, kas nav minēti 1. punktā, pārzinis vai apstrādātājs, vai apvienības un citas struktūras, kas pārstāv pārziņu vai apstrādātāju kategorijas, var iecelt vai – ja tas jādara saskaņā ar Savienības vai dalībvalsts tiesību aktiem – ieceļ datu aizsardzības speciālistu. Datu aizsardzības speciālists var rīkoties šādu apvienību un citu struktūru, kas pārstāv pārziņus vai apstrādātājus, uzdevumā.

5. Datu aizsardzības speciālistu ieceļ, pamatojoties uz viņa profesionālo kvalifikāciju, jo īpaši speciālām zināšanām datu aizsardzības tiesību un prakses jomā un spēju pildīt 39. pantā minētos uzdevumus.

6. Datu aizsardzības speciālists var būt pārziņa vai apstrādātāja darbinieks, vai viņš var veikt uzdevumus, pamatojoties uz pakalpojumu līgumu.

7. Pārzinis vai apstrādātājs publisko datu aizsardzības speciālista kontaktinformāciju un paziņo to uzraudzības iestādei.

38.pants

Datu aizsardzības speciālista statuss

1. Pārzinis un apstrādātājs nodrošina, ka datu aizsardzības speciālists tiek pienācīgi un laikus iesaistīts visos jautājumos saistībā ar personas datu aizsardzību.

2. Pārzinis un apstrādātājs atbalsta datu aizsardzības speciālistu 39. pantā minēto uzdevumu izpildē, nodrošinot resursus, kas nepieciešami, lai veiktu minētos uzdevumus, un nodrošinot piekļuvi personas datiem un apstrādes darbībām, un lai viņš uzturētu speciālās zināšanas.

3. Pārzinis un apstrādātājs nodrošina, ka datu aizsardzības speciālists nesaņem nekādus norādījumus attiecībā uz minēto uzdevumu veikšanu. Pārzinis vai apstrādātājs viņu neatlaiž vai viņam nepiemēro sankcijas par viņa uzdevumu

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

veikšanu. Datu aizsardzības speciālists ir tieši atbildīgs pārziņa vai apstrādātāja augstākās vadības priekšā.

4. Datu subjekti var vērsties pie datu aizsardzības speciālista visos jautājumos, kas saistīti ar viņu personas datu apstrādi un šajā regulā paredzēto tiesību īstenošanu.

5. Datu aizsardzības speciālistam ir saistoša slepenības vai konfidencialitātes ievērošana saistībā ar viņa uzdevumu pildīšanu, kā paredzēts Savienības vai dalībvalstu tiesību aktos.

6. Datu aizsardzības speciālists var pildīt citus uzdevumus un pienākumus. Pārzinis vai apstrādātājs nodrošina, lai neviens no minētajiem uzdevumiem un pienākumiem neradītu interešu konfliktu.

39.pants

Datu aizsardzības speciālista uzdevumi

1. Datu aizsardzības speciālistam ir vismaz šādi uzdevumi:

(a) informēt un konsultēt pārzini vai apstrādātāju un darbiniekus, kuri veic apstrādi, par viņu pienākumiem saskaņā ar šo regulu un ar citiem Savienības vai dalībvalstu noteikumiem par datu aizsardzību;

(b) uzraudzīt, vai tiek ievērota šī regula, citi Savienības vai dalībvalstu noteikumi par datu aizsardzību un pārziņa vai apstrādātāja politika saistībā ar personas datu aizsardzību, tostarp pienākumu sadali, apstrādes darbībās iesaistīto darbinieku informēšanu un apmācību, un ar to saistītajām revīzijām;

(c) pēc pieprasījuma sniegt padomus attiecībā uz novērtējumu par ietekmi uz datu aizsardzību un pārraudzīt tā īstenošanu saskaņā ar 35. pantu;

(d) sadarboties ar uzraudzības iestādi;

(e) būt par uzraudzības iestādes kontaktpunktu jautājumos, kas saistīti ar apstrādi, tostarp 36. pantā minēto iepriekšējo apspriešanos, un attiecīgā gadījumā konsultēt par jebkuru citu jautājumu.

2. Datu aizsardzības speciālists, pildot savus uzdevumus, pienācīgi ņem vērā ar apstrādes darbībām saistīto risku, ņemot vērā apstrādes raksturu, apjomu, kontekstu un nolūku.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

2. DAS IECELŠANA

2.1. Obligāta iecelšana saskaņā ar VDAR

2.1.1. Publiska iestāde vai struktūra

VDAR nesatur juridisku definējumu, kas ir "publiska iestāde vai struktūra". Tam, vai konkrēta fiziska vai juridiska persona ir publiska iestāde vai struktūra, būtu jābūt noteiktam saskaņā ar attiecīgās dalībvalsts tiesību aktiem. Šis jēdziens jāinterpretē **plaši** un jebkurā gadījumā ietver valsts, reģionālās un **vietējās varas iestādes**. Tomēr saskaņā ar DG29 tas var ietvert arī noteiktas fiziskas vai juridiskas personas, kuru darbību regulē valsts vai privātās tiesības (piemēram, sabiedriskā transporta pakalpojumi, ūdensapgāde un energoapgāde, ceļu infrastruktūra, sabiedriskā apraide, valsts mājokļi vai reglamentētu profesiju disciplinārās iestādes)[1]. Šādas interpretācijas loģika ir tāda, ka pilsoņiem (datu subjektiem) ir ierobežota izvēle, vai un kā šādas iestādes apstrādās viņu personas datus. Lai gan šāda interpretācija nav obligāta un saistoša, šīm iestādēm ieteicams rūpīgi izskatīt un izanalizēt, vai tām iecelt DAS.

Jāatzīmē, ka DG29 kā labu praksi iesaka iecelt DAS, kura funkcijām vajadzētu attiekties arī uz visām veiktajām apstrādes darbībām, tostarp tām, kas nav saistītas ar publiskā uzdevuma veikšanu vai oficiālu pienākumu izpildi (piemēram, attiecības ar darbiniekiem)[2]. Tomēr nevienā no VDAR noteikumiem nav minēta prasība iecelt DAS tikai tām apstrādes darbībām, kas saistītas ar publiskām funkcijām. Tādējādi saprātīgākā un drošākā interpretācija ir tāda, kurā pašvaldības ieceļ DAS, **kurš ir atbildīgs par visām organizācijas datu apstrādes darbībām** (attiecības ar iedzīvotājiem, darbiniekiem, kandidātiem uz darba vietām, bijušajiem darbiniekiem, citām publiskām iestādēm utt.).

2.1.2. Pārziņa vai apstrādātāja pamatdarbība […], kurai nepieciešama regulāra un sistemātiska datu subjektu novērošana plašā mērogā

Pašvaldību veiktā datu apstrāde galvenokārt notiek augstākminētā 2.1.1. punkta ietvaros, t.i., pašvaldībām būtu jāieceļ DAS, balstoties uz to publiskās iestādes vai struktūras kapacitāti. Skaidrības labad turpmāk tiks veikta īsa analīze par divām citām hipotēzēm saskaņā ar VDAR, kad DAS iecelšana ir obligāta. Šī informācija varētu būt noderīga privātām struktūrām, kuru kapitāls daļēji vai pilnīgi pieder pašvaldībai vai citām pašvaldību vai valsts struktūrām un kuras neietilpst "publiska iestāde vai struktūra" darbības laukā.

Ar terminu **"pamatdarbība"** var uzskatīt galvenās darbības, kas nepieciešamas, lai sasniegtu pārziņa vai apstrādātāja mērķus[3]. DG29 sniegtie piemēri ietver veselības datu apstrādi slimnīcās vai privātās apsardzes uzņēmuma veikto uzraudzību. No otras puses,

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

darbinieku standarta IT atbalsta pasākumi tiek izslēgti no organizācijas "pamatdarbībām"[4].

Jēdziens **"plašs mērogs"** nav skaidri definēts VDAR. Tajā ir skaidri norādīts, ka datu apstrāde reģionālā, valsts vai starpvalstu līmenī, kas ietver ievērojamu datu apjomu un kas var ietekmēt lielu datu subjektu skaitu un izraisīt augstu risku, var uzskatīt par "plaša mēroga" apstrādi. No otras puses, tādi speciālisti kā veselības aprūpes speciālists vai advokāts neapstrādā personas datus "plašā mērogā".

Saskaņā ar DG29, par plaša mēroga apstrādi var uzskatīt sekojošus piemērus:

- pacienta datu apstrāde slimnīcā;
- personu, kuras izmanto pilsētas sabiedrisko transportu, pārvietošanās datu apstrāde (piemēram, izsekošana ar braukšanas kartēm);
- starptautiskas ātrās ēdināšanas ķēžu klientu faktiskās ģeogrāfiskās atrašanās vietas datu apstrāde statistikas vajadzībām, ko veic šo pakalpojumu sniegšanas speciālists;
- klientu datu apstrāde, ko veic apdrošināšanas sabiedrība vai banka;
- personas datu apstrāde meklētājprogrammas paradumorientētai reklāmai
- datu apstrāde (saturs, transports, atrašanās vieta) pa tālruni vai caur interneta pakalpojumu sniedzējiem[5].

Jēdziens **"regulārs"** būtībā ir saistīts ar apstrādi, kas notiek vai nu pastāvīgi vai periodiski. Jēdziens **"sistemātiska novērošana"** paģērē, lai apstrāde notiktu pēc konkrēta plāna, stratēģijas vai līdzīgas iepriekš noteiktas metodoloģijas organizētā veidā saskaņā ar sistēmu[6]. Kā piemēri ir telekomunikāciju tīklu operatori, profilēšana, paradumorientēta reklāma, viedās ierīces utt.

2.1.3. Pārziņa vai apstrādātāja pamatdarbības ietver īpašo kategoriju datu […] un personas datu par sodāmību un pārkāpumiem apstrādi plašā mērogā

Jēdzienu “pamatdarbība” un “plašs mērogs” skaidrojumus skatiet augstāk punktā 2.1.2.

Vārds “un” interpretējams korektīvi kā "vai". Citiem vārdiem sakot, DAS iecelšana būtu nepieciešama organizācijā, kurā notiek īpašu kategoriju datu apstrāde **vai** personas datu par sodāmību un pārkāpumiem apstrāde plašā mērogā un kas ir organizācijas pamatdarbības daļa.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

Īpašu kategoriju personas dati ir:

- personas dati, kuri atklāj rases vai etnisko piederību;
- politiskie uzskati;
- reliģiskā vai filozofiskā pārliecība;
- dalība arodbiedrībā;
- ģenētiskie dati;
- biometriskie dati, lai veiktu fiziskas personas viennozīmīgu identifikāciju;
- dati, kas attiecas uz veselību vai fiziskas personas dzimumdzīvi vai seksuālo orientāciju.

Personas dati par sodāmību un pārkāpumiem var ietvert informāciju, kas iekļauta tiesas spriedumos, sodāmības reģistrā, izmeklēšanas dienestu aktos.

2.2. DAS iecelšana citās situācijās

2.2.1. Obligātā iecelšana saskaņā ar ES vai dalībvalstu tiesību aktiem

Saskaņā ar VDAR 37.panta 4.punktu ES un/vai dalībvalstīm ir tiesības paredzēt citas situācijas, kad DAS iecelšana ir obligāta. Šāda obligāta iecelšana var būt nepieciešama pēc kvalitatīvām pazīmēm (piemēram, noteiktām nozarēm raksturīgām apstrādes darbībām) vai kvantitatīvām pazīmēm (piemēram, ja organizācija apstrādā personas datus noteiktam skaitam datu subjektu). Piemēram, Vācija savos datu aizsardzības tiesību aktos ir noteikusi plašākas prasības nekā VDAR: a) uzņēmumiem, kas veic uzņēmējdarbību Vācijā un iesaista vismaz 10 personas automatizētas apstrādes jomā, ir obligāti jāieceļ DAS; b) automatizētas apstrādes gadījumos, kas tiek veiktas uzņēmējdarbības gaitā datu pārsūtīšanas nolūkā, anonimizētai pārsūtīšanai, tirgum vai viedoklim, uzņēmumiem ir jāieceļ DAS neatkarīgi no personu skaita, kas tiek nodarbināti personas datu automatizētai apstrādei[7].

2.2.2. Brīvprātīga iecelšana

VDAR paredz arī iespēju brīvprātīgi iecelt DAS. Šādu pieeju varētu izmantot organizācijas, kuras vēlas parādīt savu atbilstību datu aizsardzības noteikumiem un veicināt pārredzamību un uzticēšanos. Tā kā pašvaldību darbība ietilpst pirmajā obligātajā prasībā (publiska iestāde vai struktūra), brīvprātīgu DAS iecelšanu var piemērot noteiktām organizācijām, kuru kapitāls pieder pašvaldībai vai valstij, piemēram, sabiedriskā transporta uzņēmumi, valsts skolas vai universitātes, sabiedrisko pakalpojumu sniedzēji (ūdens, gāze, elektroapgāde) u.c.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

2.3. Līgumiskās attiecības ar DAS

2.3.1. Darba līgums

VDAR skaidri paredz iespēju iecelt DAS uz darba līguma pamata. Tas nozīmē divas iespējas: a) iecelt kādu personu, kas jau strādā organizācijā, apvienojot savas funkcijas ar DAS funkcijām vai b) izveidot DAS jaunu darba vietu. Izvēle starp šīm divām iespējām lielā mērā ir atkarīga no organizācijas struktūras, darbinieku skaita, darba slodzes un datu apstrādes veida un skaita, un būtu jāveic katram gadījumam atsevišķi. Ja kādas pašvaldības iestāde ir salīdzinoši maza (piemēram, atrodas mazā ciemā ar nelielu skaitu iedzīvotāju, kuru dati tiek apstrādāti), varētu būt pamatoti nepieņemt jaunu darbinieku, bet drīzāk piešķirt DAS funkcijas kādam, kas jau strādā organizācijā (jebkurā gadījumā jāizvairās no interešu konflikta). Gluži pretēji, ja pašvaldības iestāde ir liela un/vai tās ikdienas darbības saistītas ar ievērojamu personas datu apjomu (vai konfidenciālu datu vai datu saistībā ar sodāmību un pārkāpumiem) apstrādi, izvēle izveidot jaunu darba vietu (vismaz) vienam DAS šķiet pamatota.

2.3.2. Pakalpojuma līgums

VDAR neuzliek par pienākumu organizācijām iecelt DAS tikai kā personāla locekļus. Regulā ir skaidri noteikts, ka DAS funkciju var veikt arī ārpakalpojuma sniedzējs (persona vai organizācija), ar kuru noslēgts pakalpojuma līgums. DG29 iesaka par labu praksi ārējai DAS komandai noteikt katram klientam vienu vadošo kontaktpersonu un "atbildīgo personu", kas būtu jānorāda pakalpojuma līgumā[8]. Turklāt ikvienam ārējās DAS organizācijas loceklim jāatbilst visām VDAR piemērojamajām prasībām.

Ārpakalpojuma sniedzēja piesaistīšana DAS funkciju veikšanai varētu būt saprātīga arī tāpēc, ka šādai organizācijai ir nepieciešamās ekspertu zināšanas, pieredze un visi atbilstošie sertifikāti[9].

Visbeidzot, bet ne mazāk svarīgi, atkarībā no vietējās likumdošanas (piemēram, saskaņā ar publisko iepirkumu likumiem) pakalpojuma līguma noslēgšanai ar ārēju DAS varētu būt nepieciešama dažu formālu procedūru veikšana.

3. DAS AMATS

3.1. Iesaistīšana visos jautājumos, kas saistīti ar personas datu aizsardzību

VDAR skaidri nosaka, ka DAS jāiesaista visos jautājumos, kas saistīti ar personas datu aizsardzību organizācijā. DG29 saredz DAS iesaisti (konsultāciju, padomu, kontroles u.c. veidā) pēc iespējas ātrāk katrā procesā, kas ietver personas datu apstrādi, kā vienu no līdzekļiem, lai nodrošinātu konfidencialitāti saskaņā ar integrēto datu aizsardzības pieeju[10].

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

Praktiski DAS iesaistīšana organizācijā varētu iekļaut piemēram:

- Padoma lūgšana, veicot novērtējumu par ietekmi uz datu aizsardzību (NIDA) (VDAR 35.panta 2.punkts);
- Dalība darba sanāksmēs (DG29 nosaka piedalīšanos augstākā un vidējā līmeņa vadības sanāksmēs, taču praksē DAS mijiedarbībai ar personālu ekspertu līmenī varētu būt līdzīga (ja ne augstāka) pievienotā vērtība);
- Konsultēšanās ar DAS ikreiz, kad tiek pieņemts vadības lēmums saistībā ar datu apstrādi;
- Konsultēšanās ar DAS par to, kādi pasākumi jāveic, ja rodas datu aizsardzības pārkāpums.

3.2. Nepieciešamo resursu un neatkarības nodrošināšana

DAS nespētu pilnvērtīgi pildīt savus pienākumus, ja tas nebūtu nodrošināts ar nepieciešamajiem resursiem. Tāpēc organizācijas vadība ir atbildīga par to, lai DAS būtu pienācīgi nodrošināti šādi aspekti:

- **Orgnizatoriskie aspekti:**
  - DAS, veicot savas pienākumus, nepieciešama komanda, kas to atbalsta. Tas ir īpaši svarīgi lielākām organizācijām. Dažkārt vairāku DAS iecelšana varētu būt risinājums;
  - Piekļuve visām citām komandām organizācijā. DAS nespētu pienācīgi pildīt savus pienākumus, ja tas nevarētu pilnvērtīgi sadarboties ar visām citām ar datu apstrādi atbildīgajām grupām (piemēram, reģistru nodaļa un lietvedības departaments, juridiskais departaments, personāla daļa, grāmatvedība, IT departaments u.c.);
  - Atbildīgs tikai augstākās vadības priekšā. VDAR skaidri nosaka, ka DAS uzņemas atbildību tikai pret augstāko organizācijas vadību. Pašvaldību gadījumā tas varētu būt, piemēram, domes priekšsēdētājs, novada dome, attiecīgās administratīvās vienības direktors vai priekšsēdētājs utt. Šī prasība ir ļoti svarīga, lai nodrošinātu DAS neatkarību. Ja DAS saikne ar vadību būtu netieša (piemēram, izmantojot tādus starpniekus kā juridisko vai personāla daļas vadītāju), DAS nevarētu pienācīgi pildīt savus pienākumus, jo rastos situācija, kurā DAS ir atbildīgs pret kāda, kuru tam vajadzētu kontrolēt;
  - Pietiekams laiks, lai veiktu savus pienākumus. Tas ir īpaši svarīgi, ja DAS tiek iecelts uz nepilnu darba laiku, vai, ja darbinieks papildus citiem pienākumiem veic datu aizsardzību[11]. Kā labo praksi DG29 iesaka noteikt procentuālu laika daļu DAS pienākumiem, ja tā nav pilna slodze.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

- **Finanšu aspekti**
  - DAS jābūt pieejamiem nepieciešamajiem finanšu resursiem, lai veiktu savas funkcijas. Ja organizācija nenodrošina pietiekamu budžetu datu aizsardzības pasākumiem, tas varētu apdraudēt DAS funkciju pienācīgu izpildi;
  - DAS jābūt pieejamai nepieciešamajai infrastruktūrai (telpām, datoriem, interneta pieslēgumam, datu bāzēm, tehniskajiem risinājumiem, piemēram, programmatūrām u.c.).
- **Izglītības aspekti** – DAS ekspertu zināšanu līmenis būtu pastāvīgi jāpaaugstina (izmantojot kursus, nodrošinot jaunu literatūru utt.). Ņemot vērā to, ka datu aizsardzība ir ļoti dinamiska zināšanu joma, ir saprotams, ka DAS jābūt informētam par jaunākajām tendencēm un attīstību, lai pienācīgi nodrošinātu pēc iespējas augstāku datu aizsardzības līmeni organizācijā un risinātu aktuālās problēmas tehnoloģiskās un juridiskās attīstības kontekstā.

Būtisks DAS neatkarības aspekts ir **aizliegums sodīt vai radīt jebkādas nelabvēlīgas sekas** DAS par savu pienākumu pildīšanu. Nelabvēlīgas sekas var atšķirties dažādās situācijās - no atlaišanas no darba vai cita veida disciplinārsoda līdz atteikumam par paaugstināšanu amatā, atteikums par pabalstiem, ko saņēmuši citi darbinieki utt. Var sagaidīt, ka dalībvalstis savā darba likumdošanā ieviesīs grozījumus un nodrošinās DAS aizsardzību pret atlaišanu laikā, kad tie pilda savas funkcijas, un kādu laika posmu pēc tam[12]. Tajā pašā laikā būtu jāpiemēro saprātīga šā aizlieguma interpolācija - DAS nevar sodīt par pienācīgu savu pakalpojumu sniegšanu. Tomēr, ja DAS trūkst nepieciešamo zināšanu un prasmju, tie veic disciplinārus pārkāpumus utt., organizācijām jābūt tiesīgām tos atlaist, pamatojoties uz jebkuru atlaišanas iemeslu, kas minēts attiecīgajā nacionālajā darba likumdošanā.

3.3. Interešu konflikts

Ja DAS ir norīkots saskaņā ar darba līgumu, šim norīkojumam nevajadzētu radīt interešu konfliktu. Interešu konflikts varētu rasties, ja DAS pilda citus pienākumus organizācijā, kas nosaka datu apstrādes mērķus un līdzekļus iekšējā procesā. Citiem vārdiem sakot, DAS nevar būt vienlaikus direktors, izpilddirektors, finanšu vadītājs, galvenais ārsts, mārketinga nodaļas vadītājs, personāldaļas vadītājs vai IT nodaļas vadītājs[13]. Turklāt citi zemāki amati organizatoriskajā struktūrā arī var izraisīt interešu konfliktu, ja šādu pozīciju vai amatu ietvaros var tikt noteikti datu apstrādes mērķi un līdzekļi (piemēram, grāmatvedis, juridiskais konsultants, IT speciālists).

Interešu konflikts var rasties ne tikai, ja tiek noteikts DAS saskaņā ar darba līgumu, bet arī ārēja DAS gadījumā. Ja DAS tiek lūgts pārstāvēt datu pārzini vai apstrādātāju tiesā

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

lietā, kas saistīta ar datu aizsardzības jautājumiem, var rasties interešu konflikts, jo pārzinim un apstrādātājam ir pretrunīgas intereses.

4. DAS UZDEVUMI

4.1. Uzraudzība

Viens no galvenajiem DAS uzdevumiem ir uzraudzīt visas datu apstrādes darbības organizācijā. Tas būtībā ir saistīts ar informācijas saņemšanu/apkopošanu, šīs informācijas iekšēju analīzi, kā arī paskaidrojumu, ieteikumu un padomu sniegšanu organizācijā. Uzraudzības funkcija ir vērsta uz iekšējiem procesiem organizācijā, tādēļ būtu jāinformē un jāsniedz padomi ne tikai vadībai, bet arī pastāvīgajiem darbiniekiem ekspertu līmenī, kuru pienākumi ir saistīti ar personas datu apstrādi.

4.2. Novērtējums par ietekmi uz datu aizsardzību (NIDA)

VDAR nosaka, ka DAS tiek iesaistīts ar savām padomdevēja funkcijām NIDA. DG29 iesaka kā paraugpraksi lūgt DAS padomu par vienu vai vairākiem sekojošiem ar ietekmes novērtējumu saistītajiem jautājumiem:

- vai NIDA vispār ir jāveic;
- kāda metodika jāievēro, veicot NIDA;
- vai veikt iekšējo NIDA vai izmantot ārpakalpojumus;
- kādus drošības pasākumus (ieskaitot tehniskos un organizatoriskos pasākumus) piemērot, lai mazinātu datu subjektu tiesību un interešu riskus;
- vai NIDA ir ticis pareizi veikts un vai tā secinājumi ir saskaņā ar VDAR[14].

Ja organizācijas vadība nolemj neņemt vērā DAS padomus, pārskatatbildības principa ietvaros ir ieteicams dokumentēt šo lēmumu un tā iemeslus, kā arī iesniegt šo dokumentāciju uzraudzības iestādēm revīzijas gadījumā.

4.3. Kontaktpunkts

DAS ir galvenais kontaktpunkts gan uzraudzības iestādēm (VDAR 39.panta 1.punkta e) apakšpunkts), gan datu subjektiem (VDAR 38.panta 4.punkts) attiecībā uz jebkuru jautājumu, kas saistīts ar datu aizsardzību organizācijā. Tādēļ ir ļoti svarīgi pienācīgi sniegt DAS kontaktinformāciju uzraudzības iestādei un datu subjektiem. Turklāt prasība sniegt DAS kontaktinformāciju ir viens no pārredzamības principa elementiem saskaņā ar VDAR 12., 13. un 14.pantu.

VDAR neizslēdz, ka DAS izmanto iespēju konsultēties ar uzraudzības iestādēm par jebkuru jautājumu, kas saistīts ar datu aizsardzību organizācijā.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

4.4. Datu uzglabāšana

Lai gan pienākums reģistrēt apstrādes darbības ir paredzēts tikai datu pārziņiem un apstrādātājiem, nevis DAS, tomēr VDAR neaizliedz organizācijām uzticēt šo funkciju DAS. VDAR noteikts DAS **obligāto uzdevumu saraksts**, tādēļ organizācijām pēc saviem ieskatiem ir tiesības deleģēt jebkādus citus uzdevumus DAS. DG29 uzskata, ka šāda pienākuma nodošana DAS ir viens no instrumentiem, kas ļauj tam pildīt savus pienākumus, lai uzraudzītu atbilstību, informējot un konsultējot datu pārzini vai apstrādātāju[15]. Tā kā šis reģistrs ir efektīvs instruments pārskatatbildības nodrošināšanai, būtu pamatoti deleģēt šo pienākumu DAS.

5. SECINĀJUMI UN PRAKTISKIE PADOMI

DAS ir viena no galvenajām personām, kas nodrošina atbilstību jaunajiem datu aizsardzības noteikumiem. DAS loma lielā mērā ir atkarīga no pašas attiecīgās organizācijas. Ja organizācija pienācīgi iesaistīs DAS visos ar datu aizsardzību saistītos jautājumos un nodrošinās nepieciešamos resursus, lai tas varētu veikt savas funkcijas, DAS varētu būt viens no noteicošajiem faktoriem, lai nodrošinātu atbilstību un veicinātu uzticēšanos sabiedrībā. Pretējā gadījumā DAS būs diezgan ilūziska figūra, kurai nav reālas funkcijas kā vien pārvaldīt ar datu aizsardzību saistīto saziņu, kas nav šī amata būtība saskaņā ar VDAR.

Pašvaldībām ir svarīgi iecelt kvalificētus DAS, kas, ņemot vērā sagatavoto personu trūkumu ES līmenī, varētu izrādīties sarežģīts uzdevums. Jebkurā gadījumā nākamie daži gadi noteiks, kā DAS loma attīstīsies. Sabiedrībai būtu pozitīvi, ja pašvaldības būtu viens no vadošajiem piemēriem attiecībā uz to, kā vislabāk izmantot DAS.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

6. ĀRĒJIE AVOTI UN TĪMEKĻA VIETNES

Grāmatas

- **Harting, N.** Datenschutz-Grundverordnung: Das neue Datenschutzrecht in der betrieblichen Praxis, Verlag Dr. Otto Schmidt KG, Köln, 2016;
- **Voigt, P., von dem Bussche, A.** The EU General Data Protection Regulation (GDPR) – A Practical Guide, Springer International Publishing (2017);
- **Boardman, R., Mullock, J., Mole, A.** Bird & Bird Guide to General Data Protection Regulation (2016);
- **EU** General Data Protection Regulation (GDPR). An Implementation and Compliance Guide, IT Governance Publishing, Cambridgeshire (2016);

29.panta darba grupas dokumenti

- DG29, Vadlīnijas par datu aizsardzības speciālistiem (DAS), WP 243;

Tīmekļa saites

- http://europa.eu/rapid/press-release_IP-18-386_en.htm
- https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en

7. ATSAUCES

[1] DG29, Vadlīnijas par datu aizsardzības speciālistiem (DAS), WP 243, 6.lpp.
[2] Turpat
[3] Turpat
[4] Turpat, 6-7.lpp.
[5] Turpat, 8.lpp.
[6] Precīzu DG29 interpretāciju skatiet DG29, Vadlīnijas par datu aizsardzības speciālistiem (DAS), WP 243, 8.lpp.
[7] Demmel, A. The New German Federal Data Protection Act, Squire Patton Boggs, URL: <https://www.squirepattonboggs.com/~/media/files/insights/publications/2017/09/the-new-german-federal-data-protection-act/27836--german-federal-data-protection-alert.pdf> (26.03.2018);
[8] DG29, Vadlīnijas par datu aizsardzības speciālistiem (DAS), WP 243, 12.lpp.
[9] EU General Data Protection Regulation (GDPR). An Implementation and Compliance Guide, IT Governance Publishing, Cambridgeshire (2016), p. 58.
[10] DG29, Vadlīnijas par datu aizsardzības speciālistiem (DAS), WP 243, 13.lpp.
[11] Turpat, 14.lpp.
[12] Vācija jau ieviesusi DAS aizsardzību pret atlaišanu, kā arī vienu gadu pēc amata izbeigšanas, izņemot ārkārtas izbeigšanas iemeslus. Skatiet Demmel, A. The New German Federal Data Protection Act, Squire Patton Boggs, URL: <https://www.squirepattonboggs.com/~/media/files/insights/publications/2017/09/the-new-german-federal-data-protection-act/27836--german-federal-data-protection-alert.pdf> (26.03.2018);
[13] DG29, Vadlīnijas par datu aizsardzības speciālistiem (DAS), WP 243, 15.lpp.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

[14] Turpat, 16.lpp.
[15] DG29, Vadlīnijas par datu aizsardzības speciālistiem (DAS), WP 243, 17.lpp.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

ProLegis

Novērtējums par ietekmi uz datu aizsardzību

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

Saturs

1. Tiesiskais regulējums 3
   1.1. Vispārīgā datu aizsardzības regula (VDAR) 3
2. Kad nepieciešams NIDA? 5
   2.1. Pamati 5
   2.2. Gadījumi, kad NIDA veicams obligāti 6
      2.2.1. Papildus apsvērumi par nepieciešamību veikt NIDA 6
      2.2.2. NIDA veikšana vairāku līdzīgu apstrādes darbību kopumam 7
      2.2.3. Pozitīvie un negatīvie saraksti NIDA veikšanai 7
   2.3. Kad jāveic NIDA? 7
   2.4. NIDA pārskatīšana 8
   2.5. Apspriešanās ar datu uzraudzības iestādi saskaņā ar VDAR 36.pantu 8
3. Kas ir atbildīgs par NIDA veikšanu? 9
   3.1. Pamati 9
   3.2. Piedalīšanās NIDA 9
4. Kā veikt NIDA? 10
   4.1. Pamati 10
   4.2. NIDA īstenošana 10
   4.3. NIDA minimālais saturs 10
   4.4. NIDA process 11
   4.5. Datu subjektu vai to pārstāvju iekļaušana 13
   4.6. Ziņojums par NIDA 14
5. Secinājumi un praktiski padomi 16
6. Ārējie avoti un tīmekļa vietnes 17
   6.1. Grāmatas un publikācijas 17
   6.2. 29.panta darba grupas dokumenti 17
   6.3. Tīmekļa saites 17

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

1. Tiesiskais regulējums

1.1. Vispārīgā datu aizsardzības regula (VDAR)

35.pants

Novērtējums par ietekmi uz datu aizsardzību

1. Ja apstrādes veids, jo īpaši, izmantojot jaunās tehnoloģijas un ņemot vērā apstrādes raksturu, apjomu, kontekstu un nolūkus, varētu radīt augstu risku fizisku personu tiesībām un brīvībām, pārzinis pirms apstrādes veic novērtējumu par to, kā plānotās apstrādes darbības ietekmēs personas datu aizsardzību. Vienā novērtējumā var pievērsties tādu līdzīgu apstrādes darbību kopumam, kurām piemīt līdzīgi augsti riski.

2. Pārzinis, veicot novērtējumu par ietekmi uz datu aizsardzību, lūdz padomu no datu aizsardzības speciālista, ja tāds ir iecelts.

3. Šā panta 1. punktā minētais novērtējums par ietekmi uz datu aizsardzību jo īpaši ir vajadzīgs šādos gadījumos:

a) ar fiziskām personām saistītu personisku aspektu sistemātiska un plaša novērtēšana, kuras pamatā ir automatizēta apstrāde, tostarp profilēšana, un ar kuru pamato lēmumus, kas fiziskai personai rada tiesiskās sekas vai līdzīgi būtiski ietekmē fizisko personu;

b) 9. panta 1. punktā minēto īpašo kategoriju datu vai 10. pantā minēto personas datu par sodāmību un pārkāpumiem apstrāde plašā mērogā; vai

c) publiski pieejamas zonas sistemātiska uzraudzība plašā mērogā.

4. Uzraudzības iestāde izstrādā un publisko sarakstu ar tiem apstrādes darbību veidiem, attiecībā uz kuriem ir jāveic novērtējums par ietekmi uz datu aizsardzību saskaņā ar 1. punktu. Uzraudzības iestāde minētos sarakstus iesniedz 68. pantā minētajai kolēģijai.

5. Uzraudzības iestāde var izstrādāt un publiskot arī sarakstu ar tiem apstrādes darbību veidiem, attiecībā uz kuriem nav vajadzīgs novērtējums par ietekmi uz datu aizsardzību. Uzraudzības iestāde minētos sarakstus iesniedz kolēģijai.

6. Ja 4. un 5. punktā paredzētais saraksts ietver apstrādes darbības, kas ir saistītas ar preču vai pakalpojumu sniegšanu datu subjektiem vai ar viņu uzvedības novērošanu vairākās dalībvalstīs, vai kas var būtiski ietekmēt personas datu brīvu apriti Savienībā,

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

kompetentā uzraudzības iestāde pirms minētā saraksta pieņemšanas piemēro 63. pantā paredzēto konsekvences mehānismu.

7. Novērtējumā ietver vismaz:

a) plānoto apstrādes darbību un apstrādes nolūku, tostarp attiecīgā gadījumā pārziņa leģitīmo interešu sistemātisku aprakstu;

b) novērtējumu par apstrādes darbību nepieciešamību un samērīgumu attiecībā uz nolūkiem;

c) novērtējumu par 1. punktā minētajiem riskiem datu subjektu tiesībām un brīvībām; un

d) pasākumus, kas paredzēti risku novēršanai, tostarp garantijas, drošības pasākumus un mehānismus, ar ko nodrošina personas datu aizsardzību un uzskatāmi parāda, ka ir ievērota šī regula, ņemot vērā datu subjektu un citu attiecīgo personu tiesības un leģitīmās intereses.

8. Attiecīgo pārziņu vai apstrādātāju atbilstību 40. pantā minētajam rīcības kodeksam pienācīgi ņem vērā, novērtējot šādu pārziņu vai apstrādātāju veikto apstrādes darbību ietekmi, jo īpaši saistībā ar novērtējumu par ietekmi uz datu aizsardzību.

9. Attiecīgā gadījumā pārzinis pieprasa datu subjektu vai viņu pārstāvju viedokli par plānoto apstrādi, neskarot komerciālu vai sabiedrības interešu aizsardzību vai apstrādes darbību drošību.

10. Ja saskaņā ar 6. panta 1. punkta c) vai e) apakšpunktu veiktās apstrādes juridiskais pamats ir noteikts Savienības tiesību aktos vai tās dalībvalsts tiesību aktos, kuri ir piemērojami pārzinim, un minētie tiesību akti reglamentē konkrēto apstrādes darbību vai minēto darbību kopumu, un novērtējums par ietekmi uz datu aizsardzību jau ir veikts kā daļa no vispārējā ietekmes novērtējuma saistībā ar minētā juridiskā pamata pieņemšanu, šā panta 1.–7. punktu nepiemēro, izņemot, ja dalībvalstis uzskata, ka pirms apstrādes darbībām ir jāveic šāds novērtējums.

11. Ja vajadzīgs, pārzinis veic pārskatu, lai novērtētu, vai apstrāde notiek saskaņā ar novērtējumu par ietekmi uz datu aizsardzību, vismaz tad, ja ir izmaiņas attiecībā uz apstrādes darbību radīto risku.

89. līdz 96. apsvērums.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

VDAR 35.pants ir cieši saistīts ar 24., 25. un 32.pantu. Galvenā atšķirība starp 32.pantu un 35.pantu ir tāda, ka 32.pants (Apstrādes drošība) ir vērsts uz riskiem, kas saistīti ar nelabvēlīgiem notikumiem, piemēram, uzbrukumiem, bet novērtējums par ietekmi uz datu aizsardzību (NIDA), kas balstīts uz 35.pantu, galvenokārt **koncentrējas uz riskiem, kas izriet no regulāras datu apstrādes.**

NIDA ir svarīgs instruments datu aizsardzības īstenošanā ar tehnoloģiskiem līdzekļiem (integrēta datu aizsardzība), kā noteikts 25.panta 1.punktā. Abi ir balstīti uz piesardzības principu, t.i., lai identificētu riskus agrīnās izstrādes posmos, lai pirms datu apstrādes sistēmu ieviešanas un to darbības uzsākšanas apsvērtu piemērotus pretpasākumus.

NIDA ir līdzeklis, lai identificētu un analizētu šādus riskus. Gadījumos, kad NIDA nav obligāts, saistīto risku analīze tomēr ir nepieciešama, lai pienācīgi īstenotu 25. un 32.panta prasības. Abi panti skaidri atsaucas uz fizisko personu tiesībām un brīvībām. Veicamās riska analīzes dziļums un nepieciešamā dokumentācija ir atkarīga no apstrādes sarežģītības un riska pakāpes. Mēs iesakām riska analīzes dokumentāciju nodrošināt rakstveidā.

Integrētas datu aizsardzības principa īstenošana sniedzas ārpus riskiem, kas iepriekš noteikti vispārējā riska analīzē, un tajā ietverti lēmumi, ko šim nolūkam sistēmas izstrādātāji (privātuma inženierija) ir pieņēmuši vēlākā stadijā, īstenojot datu minimizēšanas principus.

2. Kad nepieciešams NIDA[1]?

2.1. Pamati

NIDA jāveic pirms tādas personas datu apstrādes, kas varētu apdraudēt fizisko personu tiesības un brīvības.

Principā NIDA ir jāveic jebkura veida datu apstrādei, ja vien *a priori* var noteikt, ka konkrētu datu apstrādes darbības neietekmēs fizisko personu tiesības un brīvības.

Par to, kāda veida datu apstrādei jānovērtē šādi riski izklāstīts, piemēram, 35.panta 3.punktā vai 91.apsvērumā. Šeit uzsvars tiek likts uz tā saucamo jauno tehnoloģiju izmantošanu (kas ir neskaidrs juridiskais jēdziens), kas ieviests VDAR attiecībā uz NIDA.

[1] Turpmākais teksts balstīts uz publikāciju vācu valodā: Kastelitz, M., Hötzendorfer, W., Riedl, R., Ausgewählte Fragen der Durchführung einer Datenschutz-Folgenabschätzung gemäß Art 35 DSGVO, Jahrbuch Datenschutzrecht 2017, 113ff.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

Riska novērtējumā jāņem vērā ne tikai pastāvošie riska scenāriji, bet arī nākotnes notikumu iespējamība, kas jāidentificē prognostiskā novērtējumā. Novērtējuma rezultāti ir jādokumentē.

35.panta 1.punkta pēdējais teikums kopā ar 92.apsvērumu sniedz svarīgu viedokli par NIDA nepieciešamības novērtēšanu: “Noteiktos apstākļos var būt saprātīgi un ekonomiski veikt plašāku novērtējumu par ietekmi uz datu aizsardzību, kura priekšmets nav tikai viens projekts, piemēram, ja publiskas iestādes vai struktūras vēlas izveidot vienotu lietotņu vai apstrādes platformu vai ja vairāki pārziņi plāno ieviest vienotu lietotņu vai apstrādes vidi kādā rūpniecības nozarē vai segmentā, vai kādai plaši lietotai horizontālai darbībai.”

2.2. Gadījumi, kad NIDA veicams obligāti

35.panta 3.punktā uzskaitīti gadījumi, kad NIDA veicams obligāti:

a) ar fiziskām personām saistītu personisku aspektu sistemātiska un plaša novērtēšana, kuras pamatā ir automatizēta apstrāde, tostarp profilēšana, un ar kuru pamato lēmumus, kas fiziskai personai rada tiesiskās sekas vai līdzīgi būtiski ietekmē fizisko personu;

b) 9. panta 1. punktā minēto īpašo kategoriju datu vai 10. pantā minēto personas datu par sodāmību un pārkāpumiem apstrāde plašā mērogā; vai

c) publiski pieejamas zonas sistemātiska uzraudzība plašā mērogā.

2.2.1. Papildus apsvērumi par nepieciešamību veikt NIDA

91.apsvērumā uzskaitīti citi gadījumi, kad nepieciešams veikt NIDA:

Apstrādes darbības

a) kas potenciāli ietver lielu cilvēku skaitu un/vai augsta līmeņa risku un/vai plaša mēroga tehnoloģijām saskaņā ar jaunākajiem sasniegumiem;

b) kas ietver augsta līmeņa risku un apgrūtina datu subjektiem izmantot savas tiesības;

c) ja personas dati tiek apstrādāti, lai pieņemtu lēmumus attiecībā uz konkrētām fiziskām personām pēc jebkādas ar fiziskām personām saistītu personisku aspektu sistemātiskas un plašas novērtēšanas, kuras pamatā ir minēto datu profilēšana, vai pēc īpašu kategoriju personas datu apstrādes, biometrisko datu apstrādes vai tādu datu apstrādes, kas attiecas uz sodāmību un pārkāpumiem, vai ar tiem saistītiem drošības pasākumiem.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

d) kas ietver augsta līmeņa risku, jo tās kavē attiecīgās personas īstenot savas tiesības vai izmantot pakalpojumu vai līgumu;

e) kas rada augstu risku, jo tās sistemātiski tiek veiktas plašā mērogā.

2.2.2. NIDA veikšana vairāku līdzīgu apstrādes darbību kopumam

35.panta 1.punkts nosaka, ka vienota NIDA var tikt veikts apstrādes darbību kopumam ar līdzīgu riska pakāpi. Novērtējot šādu līdzību, jāņem vērā datu apstrādes vispārējais mērķis katrā atsevišķā gadījumā. 92.apsvērumā ir norādīts, ka, apsverot ekonomiskās izmaksas, NIDA var būt tematiski plašāks, dodot dalībniekiem kādā rūpniecības nozarē vai segmentā iespēju aptvert lietotņu vai apstrādes vidi vai plaši lietotas horizontālas darbības ar vienu NIDA.

2.2.3. Pozitīvie un negatīvie saraksti NIDA veikšanai

Var pieņemt, ka uzraudzības iestādes publicēs pozitīvus vai negatīvus sarakstus, lai atvieglotu lēmuma pieņemšanu par NIDA nepieciešamību konkrētā gadījumā. Šie saraksti noteiks apstrādes veidus, kuriem nepieciešams NIDA ("pozitīvie saraksti") un gadījumi, kad nav nepieciešams NIDA ("negatīvie saraksti"). Kā daļa no regulatīvās saskaņotības, kas nodrošinātu labāku saskaņošanu visā ES, abi saraksti nacionālajām uzraudzības iestādēm jānosūta Eiropas Datu aizsardzības kolēģijai (35.panta 4.punkts),

Jāatzīmē, ka 29.panta darba grupa (DG29) iesaka veikt NIDA arī gadījumos, kad šķiet neskaidri, vai NIDA ir nepieciešams, lai izpildītu likumdošanas prasības pienācīgai datu aizsardzības nodrošināšanai.

2.3. Kad jāveic NIDA?

Kad un ar kādām metodēm veikt NIDA, nosaka pārzinis. Par NIDA neizpildīšanu ir paredzētas juridiskas sankcijas, tāpēc ieteicams sākt sagatavošanos NIDA pēc iespējas ātrākā projekta posmā. Katram departamentam vai attiecīgajiem darbiniekiem, kas iesaistīti datu apstrādē, jāuzsāk attiecīgie procesi. Ieteicama apmācība, lai palielinātu izpratni par NIDA nepieciešamību organizācijā.

Apsverot riska samazināšanas pasākumus jebkura projekta, kas saistīts ar datu apstrādi, agrīnajā stadijā, var palīdzēt birokrātiskās darbības saglabāt samērā zemā līmenī.

NIDA var palīdzēt ceļā uz atbilstošu risinājumu atrašanu un var palīdzēt, kā minēts iepriekš, efektīvi un savlaicīgi īstenot datu aizsardzības prasības, izmantojot atbilstošus tehnoloģiskos risinājumus (integrētu datu aizsardzību) un noklusējuma iestatījumu izvēli, ņemot vērā datu aizsardzību.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

Nodrošinot plašus un intensīvus sagatavošanās darbus, NIDA vadīs paredzēto projektu no agrīnās idejas posma līdz tā galīgās darbības ieviešanai un parādīs, ka NIDA procesam ir atkārtošanās raksturs.

Atvērts jautājums paliek, vai NIDA bija nepieciešams apstrādei, kas veikts pirms VDAR vispārējās piemērojamības (pirms 2018.gada 25.maija). Ņemot burtisko formulējumu ("pirms"), NIDA ir nepieciešams tikai tiem procesiem, kas tika uzsākti pēc 2018.gada 25.maija vai kas būtiski mainījušies pēc šī datuma.

Tā kā šajos gadījumos datu apstrādes sistēma jau darbojas, iepriekšēja pārbaude nav iespējama. Turklāt šīs darbības nepastāv neregulētā telpā (pieņemot, ka ir ņemti vērā visi iepriekšējā tiesiskā regulējuma noteikumi un pārskatu sniegšanas prasības).

Tomēr DG29 stingri iesaka veikt NIDA tām apstrādes darbībām, kas jau tiek veiktas, lai izvairītos no juridiskām neskaidrībām un pat juridiskām sankcijām.

2.4. NIDA pārskatīšana

Pēc tam, kad NIDA ir veikts, ierosināto pasākumu īstenošana ir jāpārskata. Ja tiek uzskatīts par nepieciešamu, iespējams, būs jāveic pašas datu apstrādes pārskatīšana, lai identificētu jebkādus jaunus ar datu apstrādi saistītos risku elementus. 89.apsvērumā ir norādīts, ka NIDA pārskatīšana var būt neieciešama savlaicīgi pēc sākotnējā novērtējuma. Veicot NIDA, dokumentācijā vajadzētu iekļaut laika posmus, pēc kuriem veicama NIDA kārtējā pārbaude vai atjaunošana nākotnē.

Jāņem vērā tehnoloģiju attīstība, jauns tiesiskais regulējums un izmaiņas apstrādes kārtībā. Ja iestājas risks, ir jāveic jauns NIDA.

Pienākums veikt NIDA ir daļa no datu pārziņa pienākumiem, dokumentējot to pārskatatbildību. Dokumentācijā un pārskatā jānorāda ne tikai informācija par veikto NIDA, bet arī jāuzskaita jebkādi iemesli, kāpēc nav pabeigts pilns NIDA vai pārtraukts NIDA pēc tam, kad konstatēti lieli riski datu subjektiem.

2.5. Apspriešanās ar datu uzraudzības iestādi saskaņā ar VDAR 36.pantu

Datu pārzinim ir jākonsultējas ar datu aizsardzības iestādi (DAI), ja NIDA atklāj augstus riskus un ja pārzinis nezina, kā veikt attiecīgus pasākumus, lai mazinātu šādus riskus. DAI ir jāreaģē uz šo pieprasījumu apspriesties četrpadsmit nedēļu laikā. Sarežģītiem un inovatīviem projektiem ir ieteicams pēc iespējas agrāk uzsākt NIDA, lai jebkuru DAI ieteikumu varētu ņemt vērā projekta plāna īstenošanā.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

3. Kas ir atbildīgs par NIDA veikšanu?

3.1. Pamati

Par NIDA veikšanu atbildīgs ir pārzinis - šajā gadījumā vietējā pašvaldība. Sākotnēji Komisijas priekšlikums bija uzticēt NIDA datu apstrādātājam, kas rīkojas pārziņa uzdevumā. Savukārt 95.apsvērums tikai prasa, lai nepieciešamības gadījumā un pēc pieprasījuma apstrādātājs palīdzētu pārzinim nodrošināt, ka tiek ievēroti pienākumi, kas izriet no NIDA veikšanas.

Tāpēc praksē būtu lietderīgi līgumā paredzēt apstrādātāja iesaisti un aktīvu atbalstīšanu NIDA procesā. Tas būtu arī saskaņā ar 28.panta 3.punkta f) apakšpunktu, kas paredz, ka līgumā par apstrādi (vai citā juridiskā aktā) jāparedz, ka apstrādātājs palīdz pārzinim nodrošināt 32. līdz 36.pantā minēto pienākumu izpildi, ņemot vērā apstrādes veidu un apstrādātājam pieejamo informāciju;

Bieži vien tikai apstrādātājam būs nepieciešamā informācija, lai novērtētu attiecīgos apstrādes aspektus. Šajā gadījumā jāņem vērā tirdzniecības un uzņēmējdarbības noslēpumu atklāšanas risks, tāpēc ieteicams iekļaut atbilstošu līguma noteikumu, kas to atrunā. Ja paredzēta datu apstrāde, ko veic kopīgi pārziņi, NIDA saskaņā ar 35.panta 1.punkta 2.daļu, var veikt arī viens no pārziņiem - tas neatbrīvo citus pārziņus no pienākumiem.

3.2. Piedalīšanās NIDA

NIDA ir jāorganizē kā projekts, un tādēļ tam vajadzētu būt aprīkotam ar nepieciešamajiem materiālajiem un cilvēkresursiem ar atbilstošu augsta līmeņa vadību. Veidojot projekta komandu, īpaša uzmanība jāpievērš projekta sarežģītībai, nepieciešamajām speciālista zināšanām un nepieciešamajām zināšanām par konkrēto projektu un tā vidi. Praksē var apvienot komandu, ko veido jurists, IT darbinieks, galvenais IT drošības speciālists, datu aizsardzības speciālists, departaments, kas pieprasījis apstrādi ("datu īpašnieks") utt.

Īpaša uzmanība tiek pievērsta tam, lai tiktu novērsti interešu konflikti. Tādējādi tie, kas nodarbojas ar datu apstrādi, nākotnē nav uzskatāmi par neatkarīgiem, bet, no otras puses, var sniegt vērtīgu ieguldījumu privātuma ietekmes novērtējuma izstrādē. Īstenošanu var veikt gan iekšējā komanda, gan pieaicinātas trešās personas. Ideālā gadījumā būtu jāiesaista neatkarīga institūcija.

Pārzinim ir jāvēršas pie datu aizsardzības speciālista pēc padoma. Saskaņā ar 39.panta 1.punkta c) apakšpunktu padomi par NIDA un tā īstenošanas uzraudzību ir datu

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

aizsardzības speciālista noteiktie pienākumi, bet tikai pēc pieprasījuma un nevis vadošā pozīcijā.

Tāpēc pārzinim ir pienākums saņemt padomu no datu aizsardzības speciālista. Kādā laikā un kādā mērā iesaistīt datu aizsardzības speciālistu, ir pārziņa lēmums. Vēlāk tam būtu jāpārskata arī gala ziņojums. Praksē ir ieteicams savlaicīgi iesaistīt datu aizsardzības speciālistu, jo viņa ekspertīze sākotnēji lieti noderēs.

Atkarībā no pārziņa organizācijas, ieteicams, lai NIDA apstiprinātu vadības līmenī vai attiecīga pilnvarota persona.

4. Kā veikt NIDA?

4.1. Pamati

Jāuzsver, ka VDAR nenosaka konkrētu veidu vai metodi, kādā izstrādāt NIDA, ko pašlaik intensīvi apspriež gan nacionālajos, gan Eiropas līmenī. DG29 norāda - lai izpildītu VDAR prasības var izmantot dažādas metodes un atsaucas uz esošo (vispārīgo vai nozaru) NIDA procesu sistēmu piemēriem, kas uzskaitīti pamatnostādņu par NIDA veikšanu 1.pielikumā[2].

4.2. NIDA īstenošana

Pārzinim principā ir brīva izvēle, kā īstenot NIDA procesu. Tādējādi to var pielāgot esošajām iekšējām procedūrām, ja pašvaldība ņem vērā četras prasības, kas ietvertas VDAR 35.panta 7.punktā no a) līdz d) apakšpunktam (sk. zemāk 4.3.punktu), kā NIDA obligātās prasības, kuras 29.panta darba grupa sīkāk skaidro, un papildus ņem vērā arī "iesaistītās puses" aspektu (sk. 35.panta 2.punktu) un datu subjektu viedokli (sk. 35.punkta 9.apakšpunkts).

4.3. NIDA minimālais saturs

VDAR 35.panta 7.punkta a) līdz d) apakšpunkti kopā ar 84. un 90.apsvērumu kā minimumu nosaka:

a) plānotās apstrādes darbības un apstrādes nolūki, tostarp attiecīgā gadījumā pārziņa leģitīmo interešu sistemātisks apraksts;

2 DG29, WP 248: Var izmantot dažādas metodikas (skatīt pamatnostādņu 1.pielikumu NIDA metodoloģiju piemēriem), lai palīdzētu īstenot VDAR izklāstītās pamatprasības.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

b) novērtējums par apstrādes darbību nepieciešamību un samērīgumu attiecībā uz nolūkiem;

c) novērtējums par 1. punktā minētajiem riskiem datu subjektu tiesībām un brīvībām; un

d) pasākumi, kas paredzēti risku novēršanai, tostarp garantijas, drošības pasākumi un mehānismi, ar ko nodrošina personas datu aizsardzību un uzskatāmi parāda, ka ir ievērota šī regula, ņemot vērā datu subjektu un citu attiecīgo personu tiesības un leģitīmās intereses.

c) un d) apakšpunkti ir VDAR tā sauktās "uz risku balstītas pieejas" izpausmes, kas attiecas ne tikai uz NIDA īstenošanu, bet arī uz VDAR 24., 25. un 32.panta kontekstu. Citiem vārdiem sakot, NIDA ir īpašs piemērs uz risku balstītai pieeja tādu datu apstrādei, kas varētu izraisīt augstu risku fizisku personu tiesībām un brīvībām, un kurai nepieciešams veikt plašāku risku novērtējumu un rast risinājumus. Principā tomēr jebkurai citai datu apstrādes pieļaujamības pārbaudei arī nepieciešams riska novērtējums, ieskaitot atbilstīgus tehniskos un organizatoriskos pasākumus, kas samazina risku, pirms tā tiek īstenota (skatīt VDAR 24.panta 1.punktu).

4.4. NIDA process

NIDA ir jāuztver kā process (ne tikai kā ziņojums), kas pēc iespējas drīzāk jāuzsāk, lai ietekmētu “projekta” izstrādi. Rezultātā novērtējums uz ietekmi gan atšķiras no audita, kas veic projekta pēckontroli, kad jau ir pārāk vēlu, lai risinātu datu aizsardzības vajadzības, kas būtu jādara NIDA.

Šobrīd ir daudz priekšlikumu NIDA procesa ieviešanai, kas vienā vai otrā veidā ir līdzīgi PIAF projekta ietvaros veiktā pētījuma rezultātiem (2012.g.)[3], kurā tika apkopotas ietekmes uz privātuma novērtējumu (IPN) metodoloģijas septiņās valstīs (tostarp "labās prakses” ieteikumi un IPN procesa galvenie elementi) ES Komisijai. Tika noteikti šādi galvenie elementi:

1. IPN nepieciešamības noteikšana (sliekšņa analīze).
2. IPN komandas un darba uzdevuma noteikšana.
3. Ierosinātā projekta apraksts (un ieinteresēto personu noteikšana).

[3] *De Hert/Kloza/Wright* (Hrsg), PIAF, Recommendations for a privacy impact assessment framework for the European Union, Deliverable D3 (2012), http://piafproject.eu/ref/PIAF_D3_final.pdf; vairāk informācijas http://piafproject.eu/Deliverables.html.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

4. Informācijas plūsmu un citu ietekmes uz privātumu faktoru analīze.
5. Konsultācijas ar ieinteresētajām personām (“stakeholders”).
6. Riska vadība (risku identificēšana un iespējamie risinājumi).
7. Tiesiskās atbilstības pārbaude.
8. Ieteikumu formulēšana.
9. Ziņojuma sagatavošana un publicēšana (piemēram, organizācijas tīmekļa vietnē).
10. Ieteikumu īstenošana.
11. Ārējais (trešās personas) novērtējums un/vai audits.
12. IPN pārskatīšana, ja attiecīgais projekts mainās (IPN atjaunināšana, ja projektā ir izmaiņas).

NIDA modelis viedajiem tīkliem un viedās uzskaites sistēmām, kas norādīts Eiropas Komisijas Ieteikumā 2014/724/ES, paredz šādus darbības soļus:[4]

1. solis Iepriekšējs novērtējums un kritēriji, kas nosaka nepieciešamību veikt NIDA
2. solis Uzsākšana
3. solis Viedo tīklu sistēmu vai lietojumprogrammu, ar ko apstrādā personas datus, identifikācija, raksturojums un apraksts.
4. solis Attiecīgo risku identificēšana.
5. solis Datu aizsardzības risku novērtējums.
6. solis Kontroles un atlikušo risku identificēšana un ieteikumi.
7. solis Dokumentēšana un NIDA ziņojuma izstrāde.
8. solis Pārskats un uzturēšana.

Jaunais ISO/IEC 29134 standarts sniedz vadlīnijas IPN veikšanai un ziņojuma struktūrai un saturam. Process ir sadalīts šādos četros apakšprocesos:

1. Sliekšņa analīze.
2. IPN sagatavošana.
3. IPN īstenošana.
4. IPN pārbaude.

Kādās un cik daļās NIDA process sadalāms, ir drīzāk gaumes jautājums. Citi ieteikumi piedāvā variācijas ar trim vai četriem posmiem, vēl citi - no sešiem līdz septiņiem

4 Komisijas ieteikums 2014/724/ES par datu aizsardzības ietekmējuma novērtējuma veidlapu viedajiem tīkliem un viedās uzskaites sistēmām, 2014.gada 10.oktobris, L 2014/300, 63.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

posmiem. Drīzāk svarīga ir procesa saprotamā struktūra un process, kurā jo īpaši tiek ņemts vērā VDAR 35.panta 7.punkts un 29. panta darba grupas ieteikumi.

4.5. Datu subjektu vai to pārstāvju iekļaušana

Saskaņā ar 35.panta 9.punktu, attiecīgā gadījumā pārzinis pieprasa datu subjektu vai viņu pārstāvju viedokli par plānoto apstrādi, neskarot komerciālu vai sabiedrības interešu aizsardzību vai apstrādes darbību drošību. Vārdu "attiecīgā gadījumā" iekļaušana rada neskaidrības par to, pie kādiem nosacījumiem jāgūst attiecīgās personas vai tā pārstāvja viedoklis un kādos gadījumos (pieļaujams) to var nedarīt.

Veids, kādā šo viedokli pieprasīt, ir konteksta sensitīvs, un 29.darba grupa atpazīst dažādus tā veikšanas veidus, piemēram, veicot pētījumu (iekšējo vai ārējo), oficiālas intervijas ar personāla pārstāvjiem vai arodbiedrībām un nosūtot aptaujas pārziņa nākamajiem klientiem. No formulējuma izriet, ka viedokli iespējams tikai iegūt, bet nav pienākuma ņemt to vērā vai prasība par (jaunas) piekrišanas saņemšanu. Tomēr pārzinim būs jāņem vērā datu subjektu vai viņu pārstāvju viedokļi novērtējumā uz ietekmi. Literatūrā ir strīdīgs jautājums par to, vai patērētāju aizsardzības biedrības var tikt apzīmētas ar terminu "pārstāvis"[5].

Jebkurā gadījumā pienākums konsultēties *expressis verbis* neskar komerciālu vai sabiedrības interešu aizsardzību vai apstrādes darbību drošību. Tāpēc pārzinis ārkārtas gadījumā var ierobežot vai atteikt pienākumu sniegt informāciju par paredzēto apstrādi attiecīgajām personām vai to pārstāvjiem saskaņā ar 35.panta 9.punktu (kas pēdējā gadījumā radīs situāciju, kad *a priori* iesaiste 35.panta 9.punkta izpratnē nebūs iespējama, jo pietiekamas informācijas esamība ir priekšnoteikums attiecīgo personu vai to pārstāvju viedokļa iegūšanai).

NIDA īstenošanai pierādījumu nolūkā ziņojumā ieteicams dokumentēt, kāpēc nav iegūts subjekta/tā pārstāvja viedoklis vai iegūts ierobežota satura viedoklis, vai iegūtais viedoklis nav ņemts vērā vai tikai daļēji ņemts vērā.

5 *Martini* in Paal/Pauly (Hrsg), Datenschutz-Grundverordnung (2016) Art 35 Rz 60; dagegen (mangels rechtlicher Verbundenheit) *Laue/Nink/Kremer*, Das neue Datenschutzrecht in der betrieblichen Praxis (2016) 245 Rz 99.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

4.6. Ziņojums par NIDA

Šajā brīdī jāatzīmē, ka NIDA ziņojums nav NIDA faktiskais mērķis, bet gan "līdzeklis mērķa sasniegšanai", lai dokumentētu procesu (iekšējo un ārējo). Ziņojumu nevajadzētu novērtēt par zemu - tas dokumentē īstenošanu un rezultātus, un, lai panāktu atbilstību, jāizvairās no "PR NIDA ziņojuma". Ziņojums var kalpot arī kā NIDA vadlīnijas un kontrolsaraksts.

Nedaudz pārsteidzoši, bet VDAR 35.pantā nav skaidras prasības sagatavot ziņojumu par NIDA veikšanu. Tomēr fakts, ka pārzinim ir dokumentācijas pienākums ir neapšaubāms un netieši izriet no VDAR 35.panta 7.punkta, kā arī no VDAR 5.panta 2.punkta (pārskatatbildība) kopā ar VDAR 24.panta 1.punktu un 36.panta 3.punkta e) apakšpunktu (kas paredz, ka pārzinis iesniedz uzraudzības iestādei " 35. pantā paredzēto novērtējumu par ietekmi uz datu aizsardzību"). Arī 35.panta 11.punktā pieprasītajam pārskatam, lai novērtētu, vai apstrāde tiek veikta saskaņā ar NIDA, nepieciešams, lai novērtējuma uz ietekmi rezultāti tiktu saglabāti. Turklāt ziņošana par IPN notiek saskaņā ar pasaules labo praksi šajā jomā (sk. sadaļu 4.1. augstāk), kas acīmredzami ir balstīta uz VDAR 35.punktā paredzēto NIDA.

Ieteicams NIDA procesā iekļaut "dzīvā dokumenta" (dokuments, kas tiek pastāvīgi rediģēts un atjaunināts) pieeju, sākot jau ar sliekšņa vērtības analīzes dokumentāciju, ja konstatēts, ka NIDA nav jāveic. Pat ja šī analīze parāda, ka NIDA nav nepieciešams un process tiek pārtraukts, pārzinis būs atbildīgs par atbilstību tam un pierādījumiem. Šo rakstisko dokumentāciju var iesniegt vadītājam jebkurā turpmākajā procesā un sekot līdzi iekšējiem apsvērumiem un novērtējumiem.

Attiecībā uz saturu NIDA ziņojumā būtībā ir noteikta procedūra (ieskaitot faktu izklāstu, sistemātiska apraksta veidā par visu testa priekšmetu - "novērtēšanas mērķis") un NIDA procesa rezultāti. Tāpat kā NIDA procesa gadījumā VDAR neparedz nekādus īpašus noteikumus NIDA ziņojuma sagatavošanā. Tomēr minimālā satura kritēriji ir noteikti DG29 pamatnostādņu WP 248 2.pielikumā, kas balstīti uz 35.panta 7.punktu. ISO/IEC 29134 iesaka sekojošu ziņojuma saturu ietekmes uz privātuma novērtējumam, koncentrējoties uz riska novērtējumu:

1. Atbilstošas privātuma prasības.
2. Darbības jomas apraksts.
3. Izmantoto riska kritēriju apraksts.
4. Īstenošanas dalībnieki.
5. Ieinteresētās puses, ar kurām notikušas konsultācijas.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

To apstiprina arī 90.apsvērums, kurā cita starpā ir teikts: "Minētajā novērtējumā par ietekmi jo īpaši būtu jāietver paredzētie pasākumi, aizsardzības pasākumi un mehānismi, kas mazina minēto risku, nodrošina personas datu aizsardzību un uzskatāmi parāda, ka šīs regulas noteikumi ir ievēroti."

Ļoti detalizētajā PIAF pētījumā IPN ziņojuma minimālais saturs ir šāds:[6]

1. Ievads un pamatinformācija, tostarp personas, kas apņēmušās veikt IPN, to kontaktinformācija un kur atrast papildu informāciju un citus palīdzības un padomu avotus.
2. Projekta, informācijas plūsmas un ietekmes uz privātumu apraksts.
3. Konsultāciju ar ieinteresētajām personām rezultāti.
4. Risku novērtējuma un risku samazināšanas posmu apraksts, ieskaitot iespējamās alternatīvas.
5. Tiesiskās atbilstības analīze.
6. Ieteikumi.
7. Pielikumi, ja nepieciešams.

Ja ir pieejams ziņojums vai projekta gala versija, var rasties jautājums par to, kas notiek ar atbildīgo personu (iekšēji), jo īpaši par to, vai kāds un kurš to "apstiprina" - praktiski svarīgs jautājums, kas paliek neminēts VDAR. Savā prakses kodeksā ICO (Informācijas lietu komisāra birojs Apvienotajā karalistē) ir skaidri noteicis: "iegūt atbilstošu apstiprinājumu organizācijā". Tā kā atbildīgajai personai ir jāveic NIDA, no tā izriet, ka NIDA ir iesaistīti attiecīgi atbildīgās personas pilnvaroti pārstāvji, un tiem ir arī galīgā atbildība. Vadības līmenim parasti būs galīgā lēmuma pieņemšanas pilnvaras par NIDA projekta priekšmetu un būtību. Minimālajā variantā projekta vadībai vai datu aizsardzības speciālistam jāziņo "augstākajam vadības līmenim", kā paredzēts VDAR 38.panta 3.punktā.

VDAR nav iekļauts pienākums publicēt NIDA, bet DG29 iesaka to publicēt (vismaz daļēji), lai palielinātu uzticību datu apstrādei un veicinātu pārredzamību. Jo īpaši publikācija ir ieteicama gadījumos, kad daļu no sabiedrības ietekmēs (plānotā) apstrāde.

6 *De Hert/Kloza/Wright* (Hrsg), PIAF, Recommendations for a privacy impact assessment framework for the European Union, Deliverable D3 (2012) 31, http://piafproject.eu/ref/PIAF_D3_final.pdf.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

5. Secinājumi un praktiski padomi

Īpaši labi finansētas regulatīvās aģentūras gadu gaitā ir izstrādājušas savu pieeju novērtējumam par ietekmi uz datu aizsardzību (NIDA). No šodienas viedokļa var sagaidīt, ka tās datu aizsardzības iestādes, kuras jau ir izstrādājušas savu modeli, izvēlas vai popularizē to, jo attiecīgajai uzraudzības iestādei ir visizteiktākās zināšanas par saviem ieteikumiem. Šobrīd pieejamo nacionālo uzraudzības iestāžu (no ES dalībvalstīm) modeļu saturs lielā daļā gadījumu tika sagatavots pirms VDAR, un tie (vēl) nav konsekventi pielāgoti VDAR prasībām vai terminoloģijai.

Tomēr ICO (Informācijas lietu komisāra birojs Apvienotajā karalistē) pievienoja savu ietekmes uz privātuma novērtējuma prakses kodeksu (2014.g.) ziņojumam (kuru vērts izlasīt) "Lielie dati, mākslīgais intelekts, datormācīšanās un datu aizsardzība" atbilstoši VDAR prasībām un terminoloģijai, kas tiek sagaidīts arī no citām datu aizsardzības iestādēm. Atklāts paliek jautājums, vai Eiropas Datu aizsardzības kolēģija (68.pants) sagatavos NIDA pamatnostādnes, ieteikumus un/vai paraugpraksi saskaņā ar 70.panta 1.punkta e) apakšpunktu.

Ieteikumi īsumā:

- Visu lēmumu dokumentēšana, jo īpaši, kāpēc NIDA nav veikts (ja piemērojams);
- Ja rodas šaubas, veiciet NIDA;
- Iekšējo un ārējo ieinteresēto personu iesaistīšana;
- Izmantojiet paraugus, labo praksi un, ja nepieciešams, līdzīgu NIDA, kas jau izveidots;
- NIDA publicēšana:
  - Īpaši ieteicams publiskām iestādēm;
  - Palielina informētību par privātumu un palielina uzticēšanos.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

6. Ārējie avoti un tīmekļa vietnes

6.1. Grāmatas un publikācijas

- ***Kastelitz, M., Hötzendorfer, W., Riedl, R***., Ausgewählte Fragen der Durchführung einer Datenschutz-Folgenabschätzung gemäß Art 35 DSGVO, Jahrbuch Datenschutzrecht 2017, 113ff.
- ***De Hert, Paul/Kloza, Dariusz/Wright, David,*** Recommendations for a privacy impact assessment framework for the European Union http://www.piafproject.eu/ref/PIAF_D3_final.pdf
- ***Wright, David/De Hert, Paul* (Ed.),** Privacy Impact Assessment, Springer Science & Business Media, Dordrecht, Heidelberg, London, New York 2012
- ***De Hert/Kloza/Wright*** (Ed.), **PIAF**, Recommendations for a privacy impact assessment framework for the European Union, Deliverable D3 (2012), http://piafproject.eu/ref/PIAF_D3_final.pdf; vairāk informācijas pieejams http://piafproject.eu/Deliverables.html.
- ***Martini in Paal/Pauly*** (Ed.), Datenschutz-Grundverordnung (2016) Art 35 Rz 60; dagegen (mangels rechtlicher Verbundenheit) Laue/Nink/Kremer, Das neue Datenschutzrecht in der betrieblichen Praxis (2016) 245 Rz 99.

6.2. 29.panta darba grupas dokumenti

- 29.darba grupa, WP 248, 2017.gada 4.aprīlī: Pamatnostādnes novērtējuma par ietekmi uz datu aizsardzību (NIDA) veikšanai un noskaidrošanai, vai apstrāde "varētu radīt augstu risku" Regulas 2016/679 izpratnē http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236

6.3. Tīmekļa saites

- Brussels Laboratory for Data Protection and Privacy Impact Assessments http://www.vub.ac.be/LSTS/dpialab/
- ICO, Big data, artificial intelligence, machine learning and data protection (2017), 99 f, https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

ProLegis

Pārredzamība

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

Saturs

1. TIESISKAIS REGULĒJUMS 4
   1.1. Eiropas Savienības līgumi 4
   1.3. VDAR 4
2. PĀRREDZAMĪBAS NOZĪME SASKAŅĀ AR VDAR 5
   2.1. Pārredzamības elementi saskaņā ar VDAR (12.pants) 5
      2.1.1. “Kodolīga, pārredzama, saprotama un viegli pieejama” 5
      2.1.2. “Skaidra un vienkārša valoda” 6
      2.1.3. Informācijas sniegšanas veids (12.panta, 1.punkts un 5.punkts “bezmaksas”). 6
   2.2. Informācija, kas jāsniedz datu subjektam (13. un 14.pants) 7
      2.2.1. Kāda informācija jāsniedz? 7
      2.2.2. Kāda papildus informācija jāsniedz? 7
      2.2.3. Kā informācija būtu jāsniedz? 8
      2.2.4. Kad sniegt informāciju? 8
      2.2.5. Kad jāpaziņo par izmaiņām pārredzamības informācijā, ko sniedz datu pārziņi? 9
   2.3. Īstenošanas kārtība 9
      2.3.1. Paziņojumi par privātumu 9
      2.3.2. “Push” un “pull” paziņojumi 9
      2.3.3. Citi "atbilstoši pasākumi" 10
      2.3.4. Vizualizācija 10
   2.4. Datu subjekta tiesību īstenošana 10
      2.4.1. Atkāpes no pienākuma sniegt informāciju 10
3. SECINĀJUMI UN PRAKTISKIE PADOMI 11
4. ĀRĒJIE AVOTI UN TĪMEKĻA VIETNES 12

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

Grāmatas 12
29.panta darba grupas dokumenti 12
Tīmekļa saites 12
5. ATSAUCES 12

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

1. TIESISKAIS REGULĒJUMS

1.1. Eiropas Savienības līgumi

Līguma par Eiropas Savienību (LES) 1.pants -> "…lēmumu pieņemšana ir cik iespējams atklāta un cik iespējams tuvināta pilsoņiem.";

LES 11.panta 2.punkts -> "Iestādes uztur atklātu, pārredzamu un pastāvīgu dialogu ar minētajām apvienībām un pilsonisko sabiedrību.";

Līguma par Eiropas Savienības darbību (LESD) 15.pants -> "*Jebkuram Savienības pilsonim […] ir tiesības piekļūt Savienības iestāžu un struktūru dokumentiem. […] Katra iestāde nodrošina sava darba pārredzamību…".*

1.2. ES Pamattiesību harta

Pārredzamība ir būtisks godprātīgas datu apstrādes principa elements. Šāda pārredzamība ir iekļauta ES Pamattiesību hartas 8. pantā.

8.pants

Personas datu aizsardzība

1. Ikvienai personai ir tiesības uz savu personas datu aizsardzību.

2. Šādi dati ir jāapstrādā ***godprātīgi****, noteiktiem mērķiem un ar attiecīgās personas piekrišanu vai ar citu likumīgu pamatojumu, kas paredzēts tiesību aktos. Ikvienam ir pieejas tiesības datiem, kas par viņu savākti, un tiesības ieviest labojumus šajos datos.*

3. Atbilstību šiem noteikumiem kontrolē neatkarīga iestāde.

1.3. VDAR

39.apsvērums

… Fiziskām personām vajadzētu būt pārredzamam tam, ka viņu personas datus vāc, izmanto, aplūko vai citādi apstrādā, un tam, kādā apjomā personas dati tiek vai tiks apstrādāti. Pārredzamības principa pamatā ir prasība, ka visa informācija un saziņa, kas saistīta ar minēto personas datu apstrādi, ir viegli pieejama un viegli saprotama un ka ir jāizmanto skaidra un vienkārša valoda. Minētais princips jo īpaši attiecas uz informāciju datu subjektiem par pārziņa identitāti un apstrādes nolūkiem, kā arī papildu informāciju, lai nodrošinātu godprātīgu un pārredzamu apstrādi attiecībā uz

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

attiecīgajām fiziskajām personām, un viņu tiesībām saņemt apstiprinājumu un paziņojumu par to, kuri viņu personas dati tiek apstrādāti…

58.apsvērums

Pārredzamības principa pamatā ir prasība, ka visa informācija, kas adresēta sabiedrībai vai datu subjektam, ir kodolīga, viegli pieejama un viegli saprotama un ka tiek izmantota skaidra un vienkārša valoda un papildus – vajadzības gadījumā – vizualizācija. Šādu informāciju var sniegt elektroniski, piemēram, darot to pieejamu sabiedrībai tīmekļa vietnē. Tas ir jo īpaši svarīgi situācijās, kad iesaistīto personu skaits un praksē izmantoto tehnoloģiju sarežģītība apgrūtina datu subjekta iespējas zināt un saprast, vai tiek vākti viņa personas dati, kas to dara un kādā nolūkā – kā piemēram, tiešsaistes reklāmas gadījumā. Ņemot vērā, ka bērniem pienākas īpaša aizsardzība, ja apstrāde attiecas uz bērnu, informācija būtu jāsniedz un saziņa jāveic tik skaidrā un vienkāršā valodā, lai bērns to varētu viegli saprast.

5.panta 1.punkta a) apakšpunkts

Personas datu apstrādes principi

1. Personas dati:

a) tiek apstrādāti likumīgi, godprātīgi un datu subjektam pārredzamā veidā ("likumīgums, godprātība un pārredzamība");

2. PĀRREDZAMĪBAS NOZĪME SASKAŅĀ AR VDAR

Pārredzamības princips ir saistīts ar godprātīguma un pārskatatbildības principiem. VDAR 5.pants (*Personas datu apstrādes principi*) uzliek par pienākumu datu pārziņiem spēt pierādīt, ka personas dati tiek apstrādāti pārredzamā veidā. Saskaņā ar 29. panta datu aizsardzības darba grupas[1] viedokli pārskatāmības mērķis ir pilnvarot datu subjektus pieprasīt datu pārziņu un apstrādātāju atbildību un kontrolēt savus personas datus[2]. Šis mērķis tiek realizēts, ieviešot īpašas praktiskas prasības, kuras jāievēro visos apstrādes posmos: pirms datu apstrādes vai tās sākumā, kad tiek vākti personas dati, un visa apstrādes perioda laikā.

2.1. Pārredzamības elementi saskaņā ar VDAR (12.pants)

2.1.1. "Kodolīga, pārredzama, saprotama un viegli pieejama"

Šīs prasības pirmās divas daļas nozīmē, ka datu pārziņiem efektīvi un īsā veidā jāsniedz informācija/jāveic saziņa, lai izvairītos no informatīvās nogurdināšanas (citiem vārdiem

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

sakot, pārslogot datu subjektus ar informāciju). Veids, kā to izdarīt, varētu būt pakāpeniska komunikācija, kurā subjekti tiek informēti par viņu tiesībām soli pa solim (piemēram, sniedzot galveno informāciju īsā paziņojumā, bet pārējo - datu vākšanas vietā). Šai informācijai jābūt atsevišķai no cita veida informācijas, kas nav saistīta ar privātumu, piemēram, līguma noteikumiem.
Prasība, ka informācija ir "saprotama", nozīmē, ka tai būtu jābūt saprotamai vidējam paredzētās auditorijas loceklim, šajā situācijā - vietējās sabiedrības vidusmēra iedzīvotājam. Datu subjektiem jāspēj iepriekš noteikt, kāds ir apstrādes apjoms un sekas. 29.panta darba grupa (DG29) iesaka datu pārziņiem nepārprotamā valodā skaidri norādīt, kādas būs apstrādes svarīgākās sekas, jo īpaši, ja šādas sekas var ietekmēt subjektu pamattiesības[3].
"Viegli pieejama" nozīmē, ka datu subjektam nevajadzētu meklēt informāciju. Tā vietā informācija būtu jāuzrāda acīmredzamā veidā, lai subjektam tā būtu pieejama bez pūlēm.

2.1.2. “Skaidra un vienkārša valoda”

Prasība pēc skaidras un vienkāršas valodas nozīmē, ka informācija jāsniedz pēc iespējas vienkāršāk, izvairoties no sarežģītiem teikumiem un sarežģītas valodas struktūras. Informāciju nevajadzētu formulēt ar abstraktiem vai neviennozīmīgiem terminiem vai pieļaut iespēju dažādām interpretācijām[4]. Personas datu apstrādes mērķim un juridiskajam pamatam jābūt skaidram. Jāizvairās no jebkāda neskaidra apstrādes nolūka formulējuma, piemēram, "pakalpojumu attīstībai nākotnē" vai "izpētes nolūkos". Datu subjektam sniegtajā informācijā nevajadzētu iekļaut pārāk juridisku, tehnisku vai specializētu valodu vai terminoloģiju[5].
Vietējām pašvaldībām būtu arī jānodrošina, ka valodas lietojums, tonis un stils, kādā tiek runāts ar bērniem, ir piemērots un rezonē ar bērniem, lai viņi spētu atpazīt, ka ziņa vai informācija tiek vērsta uz viņiem[6].

2.1.3. Informācijas sniegšanas veids (12.panta, 1.punkts un 5.punkts “bezmaksas”).

Datu pārziņi nevar iekasēt maksu no datu subjektiem par informāciju, kas sniegta saskaņā ar 13. un 14.pantu (informācija, kas jāsniedz datu subjektam) vai saziņu un darbībām, kas veiktas saskaņā ar 15.-22.pantu (datu subjektu tiesības) un 34.pantu (datu subjekta informēšana par personas datu aizsardzības pārkāpumu). Šajā noteikuma ir viens izņēmums: datu subjekta pieprasījumi ir acīmredzami nepamatoti vai pārmērīgi, jo īpaši to regulāras atkārtošanās dēļ. Šajā gadījumā pārzinis var pieprasīt saprātīgu maksu, ņemot vērā administratīvās izmaksas, kas saistītas ar informācijas vai saziņas nodrošināšanu vai pieprasītās darbības veikšanu. Ir svarīgi, lai datu pārziņi apzinātos, ka viņu pienākums ir spēt pierādīt pieprasījuma acīmredzami nepamatoto vai pārmērīgo

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

raksturu. Tāpēc pašvaldībām nav ieteicams iekasēt maksu no iedzīvotājiem par informāciju, kas sniegta saskaņā ar VDAR.

2.2. Informācija, kas jāsniedz datu subjektam (13. un 14.pants)

2.2.1. Kāda informācija jāsniedz?

VDAR 13. un 14.pants nosaka, kādu informāciju nepieciešams sniegt datu subjektam. Regulā ir atšķirība starp gadījumiem, kad dati iegūti no datu subjekta (13.pants) un kad tie nav iegūti no datu subjekta (14.pants). Vietējām pašvaldībām būtu jānodrošina:

1) Informācija par pārziņa identitāti un kontaktinformācija;
2) datu aizsardzības speciālista kontaktinformācija;
3) apstrādes nolūki un to pamatojums tiesību aktos – pašvaldībām galvenokārt pamatojums būs 6.panta, 1.punkta e) apakšpunkts: lai izpildītu uzdevumu, ko veic īstenojot pārzinim likumīgi piešķirtās oficiālās pilnvaras un attiecīgie noteikumi dalībvalsts tiesību aktos;
4) apstrādāto datu veids, ja datu subjekts tos nav sniedzis;
5) iespējamo datu saņēmēju identitāte - tajā ietilpst ne tikai trešās personas, bet arī datu apstrādātāji un kopīgi pārziņi. Definējot dažādas datu saņēmēju kategorijas, pārzinim jābūt pēc iespējas konkrētākam.

2.2.2. Kāda papildus informācija jāsniedz?

Pirmkārt, lai nodrošinātu godprātīgu un pārredzamu apstrādi, pārzinim jāinformē datu subjekts par:

1) laikposmu, cik ilgi personas dati tiks glabāti, vai kritēriji, ko izmanto minētā laikposma noteikšanai;
2) tiesībām pieprasīt no pārziņa piekļuvi datu subjekta personas datiem un to labošanu vai dzēšanu, vai apstrādes ierobežošanu attiecībā uz datu subjektu un tiesībām iebilst pret apstrādi, kā arī tiesībām uz datu pārnesamību;
3) tiesībām jebkurā brīdī atsaukt piekrišanu, ja apstrāde pamatojas uz piekrišanu;
4) tiesībām iesniegt sūdzību uzraudzības iestādei;
5) to, ka pastāv automatizēta lēmumu pieņemšana, tostarp profilēšana, un jēgpilni jāsniedz informācija par tajā ietverto loģiku, kā arī par šādas apstrādes nozīmīgumu un paredzamajām sekām attiecībā uz datu subjektu.

Informācijai par profilēšanu ir jābūt ne tikai viegli pieejamai datu subjektiem, bet tā jādara viņiem zināma. Pārzinim vajadzētu atrast vienkāršus veidus, kā informēt datu subjektu par loģiku vai kritērijiem, kas tiek izmantoti automatizētai lēmumu pieņemšanai, bez sarežģītiem algoritmu skaidrojumiem.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

Ja dati netika iegūti no datu subjekta, datu pārzinim būtu jāsniedz to avots. Ja datu subjekts sniedz datus, pārzinim jāinformē viņš vai viņa par to, vai personas datu sniegšana ir obligāta prasība.
Otrkārt, pārzinim jāinformē datu subjekti, ja viņi plāno apstrādāt datus jebkādiem citiem nolūkiem, kas atšķiras no tiem, kuriem dati tika vākti. Datu subjektiem jāsniedz informācija par šo citu nolūku un jebkāda attiecīgā papildu informācija, kas ir identiska informācijai, kas tika sniegta sākotnējam nolūkam (apstrādes periods, apstrādes juridiskais pamats utt.). Iegūstot datus, būtu lietderīgi informēt datu subjektus par iespējamu apstrādi nākotnē, ja tas visticamāk tiks veikts, ņemot vērā pārziņa darbību.

2.2.3. Kā informācija būtu jāsniedz?

Noklusētais veids, kā sniegt informāciju un sazināties ar datu subjektiem, ir rakstisks. Tomēr VDAR ļauj informāciju sniegt arī izmantojot citus līdzekļus, tostarp elektroniskos. Saskaņā ar DG29 ir svarīgi, lai izvēlētās metodes informācijas sniegšanai atbilstu konkrētiem apstākļiem[7]. Informācija pēc pieprasījuma var tikt sniegta datu subjektam mutiski, ja viņu identitātes informāciju pierāda citi (t.i., bez mutvārdu) līdzekļi[8]. Šajā noteikumā ir izņēmums attiecībā uz to informāciju, kas jāsniedz datu pārzinim saskaņā ar 13. un 14.pantu - šī informācija var tikt izpausta subjektam bez identitātes pārbaudes. Mutiskā informācijas sniegšana ne vienmēr nozīmē informāciju, ko viena persona mutiski sniedz otrai personai, tas var nozīmēt arī automatizētu mutisku informāciju. Saskaņā ar DG29, datu pārzinim vajadzētu dot iespēju datu subjektam atkārtoti noklausīties iepriekš ierakstītas ziņas, jo īpaši, ja tas attiecas uz datu subjektiem ar redzes traucējumiem vai citiem datu subjektiem, kuriem var rasties grūtības piekļūt informācijai vai izprast to rakstveidā. Arī gadījumos, kad tiek sniegta mutiska informācija, datu pārziņiem joprojām jāspēj pierādīt, ka tie ievērojuši VDAR prasības. Lai to izdarītu, viņiem būtu jānodrošina, ka viņi reģistrē 1) pieprasījumu saņemt informāciju mutiski; 2) metodi, ar kuru datu subjekta identitāte tika pārbaudīta; un 3) to, ka datu subjektam tika sniegta informācija[9].

2.2.4. Kad sniegt informāciju?

Informācija par personas datu apstrādi datu subjektam jāsniedz datu iegūšanas laikā (13.panta 1.punkts). Ja dati nav tieši iegūti no datu subjekta, bet no cita avota, informāciju datu subjektam sniedz saprātīgā termiņā, bet ne vēlāk kā viena mēneša laikā pēc datu iegūšanas, ņemot vērā konkrētos apstākļus. Pastāv divi specifiski gadījumi: pirmkārt, kad personas datus ir paredzēts izmantot saziņai ar datu subjektu, informācija jāsniedz vēlākais tad, kad ar minēto datu subjektu notiek pirmā saziņa; un, otrkārt, ja ir paredzēts datus izpaust citam saņēmējam - vēlākais tad, kad personas dati pirmoreiz tiek izpausti.
Šo periodu var pagarināt vēl uz diviem mēnešiem (kopā maksimāli trīs mēneši), ņemot vērā pieprasījumu sarežģītību un skaitu (piemēram, ja pieprasījums ietver vairākas

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

datubāzes). Viena mēneša laikā pēc pieprasījuma saņemšanas pārzinim jāinformē datu subjekts par jebkuru šādu pagarinājumu, kā arī aizkavēšanās iemesliem un par subjekta tiesībām iesniegt sūdzību.

2.2.5. Kad jāpaziņo par izmaiņām pārredzamības informācijā, ko sniedz datu pārziņi?

Gadījumos, kad informācijas apmaiņai var būt nopietna ietekme uz datu subjektu, datu apstrādātājiem jāsniedz informācija jau pirms izmaiņām, kas faktiski stājas spēkā[10]. Tas jādara skaidrā un efektīvā veidā. Personām vajadzētu būt pietiekami daudz laika, lai apsvērtu izmaiņu būtību un ietekmi un īstenotu savas tiesības attiecībā uz izmaiņām saskaņā ar VDAR, piemēram, lai iebilstu pret apstrādi. DG29 iesaka regulāri atgādināt datu subjektiem par datu apstrādes apjomu[11].
Plānojot apstrādāt datus citam nolūkam nekā tam, dēļ kura dati tika iegūti, pirms jaunās apstrādes uzsākšanas par to jāinformē datu subjekti.

2.3. Īstenošanas kārtība

Īstenošanas kārtība ir formāti, kādos datu pārziņi izpilda savus pienākumus saskaņā ar VDAR, lai sniegtu informāciju datu subjektiem.

2.3.1. Paziņojumi par privātumu

Attiecībā uz tiešsaistes platformām ir jāievēro vairāku līmeņu konfidencialitātes paziņojumu / paziņojumu pieeja, lai saistītu dažādas informācijas kategorijas, kas jānodrošina datu subjektam, nevis vienota paziņojuma izmantošana.[12]. Šī pieeja ļauj lietotājiem pāriet tieši uz to paziņojuma sadaļu, kuru viņi vēlas izlasīt. Veidojot šādu vairāku pakāpju paziņojumu, pārziņiem jācenšas nodrošināt skaidru un saprotamu pārskatu (vai saturu), lai datu subjekti zinātu, kur viņi var atrast katru informācijas daļu.

2.3.2. “Push” un “pull” paziņojumi

29.panta darba grupa arī ievieš paziņojumu "*push*" un "*pull*" izmantošanu. Galvenā atšķirība ir tāda, ka pēdējā gadījumā (“*pull*”) tiek sagaidīts, ka vietnes lietotāji paši pieprasa informāciju (šajā gadījumā informāciju par viņu datu apstrādi), bet pirmajā gadījumā (“*push*”) paziņojums "izlec" uz ekrāna bez jebkādām lietotāja darbībām. DG29 sniedz piemērus un definīcijas “*push*” paziņojumiem ar "*just-in-time*" (“tieši laikā”) pārredzamības informatīviem paziņojumiem un "*pull*" paziņojumiem - ar pārredzamības informācijas paneļiem un "*uzzini vairāk*" apmācībām[13]:

- *“Just-in-time” (“tieši laikā”)* paziņojumu izmanto, lai sniegtu konkrētu "informāciju par privātumu" brīdī, kad tas ir vispiemērotākais, lai datu subjekts varētu to izlasīt. Šis formāts var būt noderīgs, ja pašvaldības tīmekļa vietne nodrošina noteiktu

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

pakalpojumu, kas tiek veikts tiešsaistē pēc veidlapas aizpildīšanas. Pirms persona noformē veidlapu, šāds brīdinājums var parādīties ekrānā.

- *Pārredzamības informācijas panelis* ir vienīgais punkts, no kura datu subjekti var skatīt "privātuma informāciju" un pārvaldīt sava privātuma izvēles, atļaujot vai novēršot savu datu izmantošanu noteiktos veidos.

2.3.3. Citi "atbilstoši pasākumi"

Saskaņā ar DG29 atbilstoši pasākumi ārpus digitālās vides var būt:

- Papīra formātā: rakstiski paskaidrojumi, bukleti;
- Telefons: reālas personas mutvārdu paskaidrojumi, automatizēta vai iepriekš ierakstīta informācija ar iespējām dzirdēt sīkāku informāciju;
- QR kodi, balss brīdinājumi, rakstiska informācija viedajā ierīcē, nosūtītas īsziņas vai e-pasta ziņojumi un citi;
- Tiešajā saziņā: mutvārdu paskaidrojumi, rakstiski paskaidrojumi papīra vai elektroniskā formātā[14].

2.3.4. Vizualizācija

VDAR paredz vizualizācijas rīkus (jo īpaši atsaucoties uz ikonām, sertifikācijas mehānismiem un datu aizsardzības zīmogiem un marķējumiem). Ikonu ideja ir nodrošināt pieejamu informāciju datu subjektiem, izmantojot standartizētus simbolus vai attēlus, kas atzīti visā ES. "Ikonu koda" izstrāde vēl nav sākusies. VDAR arī paredz izmantot datu aizsardzības sertifikācijas mehānismus, datu aizsardzības zīmogus un marķējumus, lai parādītu atbilstību regulai. Sertifikācijas mehānismus nosaka dalībvalstis, uzraudzības iestādes, Eiropas Datu aizsardzības uzraudzītājs vai Komisija, un tie ir paredzēti, lai spētu pierādīt, ka pārzinis atbilst VDAR prasībām, parādot, ka tas īsteno tehniskos un organizatoriskos pasākumus, lai izpildītu datu aizsardzības standartus. Šie formāti var tikt piemēroti struktūrām, kas nav publiskas iestādes, piemēram, autonoms pašvaldības uzņēmums.

2.4. Datu subjekta tiesību īstenošana

Datu subjektiem ir tiesības saņemt informāciju no datu pārziņiem par saviem personas datiem. Informācija, kas jānodrošina saskaņā ar VDAR, ir skaidri norādīta regulas 13. un 14.pantā un datu subjektiem nav jāiesniedz pieprasījums vai jāveic citi aktīvi pasākumi, lai to iegūtu atšķirībā no gadījumiem, kad tiek īstenotas citas viņu tiesības (tiesības piekļūt datiem, labot vai dzēst tos u.c.).

2.4.1. Atkāpes no pienākuma sniegt informāciju

Tiesības uz informāciju nav absolūtas vai, citiem vārdiem sakot, noteiktos gadījumos tās ir ierobežotas.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

Atsevišķos gadījumos vietējās pašvaldības ir atbrīvotas no pienākuma sniegt informāciju, kas izklāstīta 6. pantā. 13 un 14. Dažos gadījumos pašvaldības ir atbrīvotas no pienākuma sniegt iepriekšminēto informāciju. Kad datus iegūst no datu subjekta, vienīgā šāda situācija ir tad, kad viņa vai viņas rīcībā jau ir attiecīgā informācija (13.panta 4.punkts). Ja dati nav iegūti no subjekta, izņēmumi ir vairāki (14.panta 5.punkts):

- informācija jau ir datu subjekta rīcībā;
- kad izrādās, ka šādas informācijas sniegšana nav iespējama vai tā prasītu nesamērīgi lielas pūles vai padarītu apstrādes mērķu sasniegšanu neiespējamu vai būtiski traucētu to sasniegšanu; piemēram, neiespējami būtu sniegt informāciju tādā gadījumā, kad pārzinim nav nekādas iespējas sazināties ar datu subjektu;
- kad iegūšana vai izpaušana ir skaidri paredzēta ES vai ES dalībvalsts tiesību aktos, kas būtu visizplatītākais nosacījums vietējām pašvaldībām;
- kad ir jāsaglabā personas datu konfidencialitāte, ievērojot dienesta noslēpuma glabāšanas pienākumu, ko reglamentē ar Savienības vai dalībvalsts tiesību aktiem, ieskaitot statūtos noteiktu pienākumu glabāt noslēpumu; šis izņēmums var būt piemērojams autonomiem pašvaldību uzņēmumiem un līdzīgām struktūrām.

Saskaņā ar DG29 šie izņēmumi parasti ir jāinterpretē un jāpiemēro šauri[15].

3. SECINĀJUMI UN PRAKTISKIE PADOMI

Pārredzamības princips ir viens no VDAR pamatiem. Daudzos veidos tas nodrošina, ka fiziskām personām pieejama visa nepieciešamā informācija, lai tās būtu informētas gan par to, kādi personas dati tiek apstrādāti par viņiem, gan par iespējām izmantot savas tiesības saskaņā ar regulu. Informācijai jābūt viegli pieejamai un viegli saprotamai skaidrā un vienkāršā valodā.

Vietējām pašvaldībām būtu ieteikums sastādīt sarakstu ar visu sniedzamo informāciju, ko pieprasa VDAR un izvēlēties vislabāko kārtību, kādā sasniegt personas, kuru datus tās apstrādā. Piemēram, tās var izveidot informācijas datu lapas un izvietot publiski pieejamos kabinetos/telpās un izveidot brošūras, kas ietver informāciju saskaņā ar 13. un 14.pantu un izplatīt tos. Elektroniskie līdzekļi var būt noderīgi, piemēram, ja organizācijai ir tiešsaistes vietne vai platforma, bet atsevišķos gadījumos var būt nepieciešami papīra formāti. Īpaša uzmanība jāpievērš gadījumos, kad pašvaldību tīmekļa vietnes piedāvā tiešsaistes pakalpojumus. Tāpat būtu jāpatur prātā, ka daži autonomi pašvaldību uzņēmumi (piemēram, sabiedriskā transporta uzņēmumi), veic dažāda veida datu apstrādes un strādā ar milzīgām datu bāzēm, tādēļ tām būtu jāpieliek īpašas pūles, lai izveidotu datu subjektiem sniedzamo informāciju korekti saskaņā ar 13. un 14.punktu.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

4. ĀRĒJIE AVOTI UN TĪMEKĻA VIETNES

Grāmatas

- **Voigt, P., von dem Bussche, A.**, The EU General Data Protection Regulation (GDPR) – A Practical Guide, Springer International Publishing (2017);
- Bird & Bird Guide to General Data Protection Regulation (2016);
- EU General Data Protection Regulation (GDPR). An Implementation and Compliance Guide, IT Governance Publishing, Cambridgeshire (2016).

29.panta darba grupas dokumenti

- 29.darba grupa, Vadlīnijas par datu aizsardzības speciālistiem (DAS), WP 243;
- 29.darba grupa, Atzinums 06/2014 par personas datu apstrādātāja likumīgo interešu jēdzienu saskaņā ar Direktīvas 95/46/EK 7. pantu, WP 217.

Tīmekļa saites

- http://europa.eu/rapid/press-release_IP-18-386_en.htm
- https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en

5. ATSAUCES

[1] 29.panta darba grupa (DG29) izveidota, pamatojoties uz 29.pantu Direktīvā 95/46/EK, kura aizstāta ar VDAR. Darba grupas mērķis ir sniegt atzinumus un ieteikumus, kā arī konsultācijas par personas datu aizsardzību.
[2] Article 29 Data Protection Working Party, Guidelines on transparency under Regulation 2016/679, p. 23.
[3] Ibid, p. 8.
[4] Ibid, p. 9.
[5] Ibid
[6] Ibid
[7] Ibid, p. 21.
[8] Ibid, p. 11.
[9] Ibid, p. 12.
[10] Ibid, p. 15.
[11] Ibid, p. 16.
[12] Ibid, p. 17.
[13] Ibid, p. 17.-18.
[14] Ibid, p. 18-19.
[15] Ibid, p. 25.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

ProLegis

Informācijas izpaušana vai datu subjekta piekļuves tiesības VDAR 15.pants

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

Saturs

1. Tiesiskais regulējums 3
   1.1. Vispārīgā datu aizsardzības regula (VDAR) 3
2. Pamati 5
3. Informācijas izpaušana datu subjektam 5
   3.1. Informācijas izpaušanas būtība 5
   3.2. Cik daudz laika ir pārzinim, lai sniegtu atbildi (termiņš)? 6
   3.3. Kādā veidā var pieprasīt informāciju un kā uz to jāatbild? 7
   3.4. Vai jāpierāda pieteikuma iesniedzēja (datu subjekta) identitāte? 7
   3.5. Maksa? Vai par informācijas sniegšanu jāatlīdzina? 8
   3.6. Vai datu subjektam ir pienākums iesaistīties informācijas izpaušanā? 8
   3.7. Vai, sniedzot informāciju, jāņem vērā trešo personu tiesības? 8
4. Pārbaudes saraksts informācijas izpaušanai pēc pieprasījuma 9
   4.1. Informācijas nosūtīšana 10
5. Ārējie avoti un tīmekļa vietnes 11
   5.1. Grāmatas un publikācijas 11
   5.2. Citi dokumenti un prakse 11

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

1. Tiesiskais regulējums

1.1. Vispārīgā datu aizsardzības regula (VDAR)

15.pants

Datu subjekta piekļuves tiesības

1. Datu subjektam ir tiesības saņemt no pārziņa apstiprinājumu par to, vai attiecībā uz datu subjektu tiek vai netiek apstrādāti personas dati, un, ja tiek, datu subjektam ir tiesības piekļūt attiecīgajiem datiem un saņemt šādu informāciju:

a) apstrādes nolūki;

b) attiecīgo personas datu kategorijas;

c) personas datu saņēmēji vai saņēmēju kategorijas, kam personas dati ir izpausti vai kam tos izpaudīs, jo īpaši saņēmēji trešās valstīs vai starptautiskās organizācijās;

d) ja iespējams, paredzētais laikposms, cik ilgi personas dati tiks glabāti, vai, ja nav iespējams, kritēriji, ko izmanto minētā laikposma noteikšanai;

e) tas, ka pastāv tiesības pieprasīt no pārziņa datu subjekta personas datu labošanu vai dzēšanu, vai personas datu apstrādes ierobežošanu vai tiesības iebilst pret šādu apstrādi;

f) tiesības iesniegt sūdzību uzraudzības iestādei;

g) visa pieejamā informācija par datu avotu, ja personas dati netiek vākti no datu subjekta;

h) tas, ka pastāv automatizēta lēmumu pieņemšana, tostarp profilēšana, kas minēta 22. panta 1. un 4. punktā, un – vismaz minētajos gadījumos – jēgpilna informācija par tajā ietverto loģiku, kā arī šādas apstrādes nozīmīgumu un paredzamajām sekām attiecībā uz datu subjektu.

2. Ja personas datus nosūta trešai valstij vai starptautiskai organizācijai, datu subjektam ir tiesības saņemt informāciju par atbilstošām garantijām, ko saistībā ar datu nosūtīšanu piemēro, ievērojot 46. pantu.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

3. Pārzinis nodrošina apstrādē esošo personas datu kopiju. Par visām papildus kopijām, ko pieprasa datu subjekts, pārzinis var iekasēt saprātīgu samaksu, kas balstīta uz administratīvām izmaksām. Ja datu subjekts pieprasījumu iesniedz elektroniskā formā un ja vien datu subjekts nepieprasa citādi, informāciju sniedz plaši izmantotā elektroniskā formātā.

4. Tiesības saņemt 3. punktā minēto kopiju neietekmē nelabvēlīgi citu personu tiesības un brīvības.

63. un 64.apsvērums:

(63) Datu subjektam vajadzētu būt tiesībām piekļūt personas datiem, kas par to savākti, un viegli un saprātīgos intervālos īstenot minētās tiesības, lai zinātu par apstrādi un pārliecinātos par tās likumīgumu. Tas ietver arī datu subjektu tiesības piekļūt saviem veselības datiem, piemēram, datiem par slimības vēsturi, kas ietver tādu informāciju kā diagnozes, analīžu rezultāti, ārstējošā terapeita vērtējums un ārstēšanas vai medicīniskās iejaukšanās pasākumi. Tāpēc katram datu subjektam vajadzētu būt tiesībām zināt un saņemt paziņojumu jo īpaši par to, kādos nolūkos personas datus apstrādā, ja iespējams, cik ilgi personas dati tiek apstrādāti, personas datu saņēmējus, kāda ir jebkurā personas datu automātiskajā apstrādē ietvertā loģika un kādas ir šādas apstrādes sekas – vismaz tad, ja apstrāde pamatojas uz profilēšanu. Ja iespējams, pārzinim būtu jāspēj nodrošināt attālināta piekļuve drošai sistēmai, kas datu subjektam sniegtu tiešu piekļuvi saviem personas datiem. Minētajām tiesībām nevajadzētu nelabvēlīgi ietekmēt citu personu tiesības vai brīvības, tostarp tirdzniecības noslēpumus vai intelektuālā īpašuma tiesības un jo īpaši autortiesības, ar ko aizsargāta programmatūra. Tomēr minēto apsvērumu rezultātam nevajadzētu būt tādam, ka datu subjektam tiek atteikts sniegt jebkādu informāciju. Ja pārzinis apstrādā lielu informācijas apjomu saistībā ar datu subjektu, pārzinim būtu jāspēj pieprasīt, lai datu subjekts pirms informācijas nosūtīšanas precizētu, uz kuru informāciju un kurām apstrādes darbībām pieprasījums attiecas.

(64) Pārzinim būtu jāizmanto visi saprātīgi pasākumi, lai pārbaudītu datu subjekta, kas izdara pieprasījumu, identitāti, jo īpaši saistībā ar tiešsaistes pakalpojumiem un tiešsaistes identifikatoriem. Pārzinim nebūtu jāglabā personas dati, ja vienīgais šādas glabāšanas nolūks ir būt spējīgam reaģēt uz iespējamiem pieprasījumiem.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

2. Pamati

VDAR 15.pants paredz, ka datu pārzinis (piemēram, uzņēmums, darba devējs, slimnīca) pēc datu subjekta (piemēram, klienta, darbinieka, darba meklētāja, pacienta, turpmāk tekstā - "datu subjekts") pieprasījuma izpauž visu informāciju, kas tam pieejama par datu subjektu. To sauc par "datu subjekta piekļuves tiesībām" (uz viņa/viņas datiem). Šo tiesību mērķis ir tāds, ka datu subjekts var iegūt informāciju par viņa vai viņas apstrādāto datu saturu un citu saistīto informāciju, lai, ja nepieciešams, varētu izmantot savas papildu datu subjekta tiesības (piemēram, labot vai dzēst datus saskaņā ar VDAR 16.pantu) vai pārliecināties par apstrādes likumību.

Šīs tiesības ir galvenais datu aizsardzības tiesību akta rīks šim mērķim, tāpēc tās uzskatāmas par pamatu datu subjekta citu tiesību izmantošanai. Lai gan datu aizsardzības iestādes (DAI) saskaņā ar VDAR ir pilnvarotas veikt pārziņa revīziju bez konkrētas sūdzības, praksē (DAI ierobežoto resursu dēļ) tā ir nepilnīga vai novēlota attiecībā uz datu subjektu piekļuves tiesībām. Pārzinim jābūt labi sagatavotam šādiem procesiem.

Vislabākais sagatavošanās veids ir labi strukturēts un pēc iespējas detalizētāks apstrādes darbību reģistrs. Jo labāk darba procesā, kam nepieciešama personas datu apstrāde, sagatavota šī dokumentācija, jo vieglāk un ātrāk pēc tam nepieciešamības gadījumā atrast konkrētus datus par konkrētu tēmu.

3. Informācijas izpaušana datu subjektam

3.1. Informācijas izpaušanas būtība

Piekļuves tiesības datu subjektam dod:

1. Tiesības jautāt pārzinim apstiprinājumu, vai viņa/viņas personas dati tiek vai netiek apstrādāti; ja nepieciešams, uz pieprasījumu jāatbild "negatīvi", ja par šo personu netiek apstrādāti dati (tā dēvētā "negatīvā atbilde"): "Mēs neapstrādājam datus par jums";
2. Tiesības iegūt apstrādājamo personas datu kopiju (jebkurai papildu datu kopijai, ko pieprasa datu subjekts, pārzinis var iekasēt saprātīgu samaksu, kas balstīta uz administratīvajām izmaksām.) Ja datu subjekts pieteikumu iesniedz elektroniski,
3. tad informāciju sniedz plaši izmantotā elektroniskā formātā, ja vien netiek pieprasīts savādāk.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

4. Tiesības iegūt šādu informāciju:

VDAR 15.panta 1.punkts	Informācijas saturs
a) apakšpunkts	**apstrādes nolūki**
b) apakšpunkts	attiecīgo personas datu **kategorijas**
c) apakšpunkts	**personas datu saņēmēji vai saņēmēju kategorijas**, kam personas dati ir izpausti vai kam tos izpaudīs, jo īpaši saņēmēji trešās valstīs vai starptautiskās organizācijās;
d) apakšpunkts	ja iespējams, **paredzētais laikposms, cik ilgi personas dati tiks glabāti**, vai, ja nav iespējams, kritēriji, ko izmanto minētā laikposma noteikšanai;
e) apakšpunkts	**ka pastāv tiesības pieprasīt no pārziņa datu subjekta personas datu labošanu vai dzēšanu, vai personas datu apstrādes ierobežošanu** vai tiesības iebilst pret šādu apstrādi;
f) apakšpunkts	**tiesības iesniegt sūdzību** uzraudzības iestādei;
g) apakšpunkts	**visa pieejamā informācija par datu avotu**, ja personas dati netiek vākti no datu subjekta;
h) apakšpunkts	ka pastāv **automatizēta lēmumu pieņemšana, tostarp profilēšana**, kas minēta 22.panta 1. un 4.punktā, un – vismaz minētajos gadījumos – jēgpilna informācija par tajā ietverto loģiku, kā arī šādas apstrādes nozīmīgumu un paredzamajām sekām attiecībā uz datu subjektu.
2.punkts	Ja personas datus **nosūta trešai valstij vai starptautiskai organizācijai**, datu subjektam ir tiesības saņemt informāciju par atbilstošām garantijām, ko saistībā ar datu nosūtīšanu piemēro, ievērojot 46. pantu.

Piezīme: Saskaņā ar 23.pantu **tiesības uz informāciju var tikt ierobežotas ar nacionālajiem tiesību aktiem.**

3.2. Cik daudz laika ir pārzinim, lai sniegtu atbildi (termiņš)?

Principā uz informācijas pieprasījumu ir jāatbild bez kavēšanās, bet ne vēlāk kā mēneša laikā pēc pieteikuma saņemšanas (VDAR 12.panta 3.punkts). Ja nepieciešams, šo periodu var pagarināt vēl uz diviem mēnešiem, ņemot vērā pieteikumu sarežģītību un skaitu. Pārzinis informē datu subjektu par termiņa pagarinājumu viena mēneša laikā pēc pieprasījuma saņemšanas, kā arī kavējuma iemeslus. Ja pieteikums ir iesniegts elektroniski, datu subjekts, ja iespējams, tiek informēts ar elektroniskiem līdzekļiem, izņemot, ja tas pieprasījis citādi.

Ja pārzinis pēc datu subjekta pieprasījumu nerīkojas, viņš/viņa bez kavēšanās, bet ne vēlāk kā vienu mēnesi pēc pieprasījuma saņemšanas, informē datu subjektu par tā iemesliem un par iespēju iesniegt sūdzību uzraudzības iestādei un vērsties tiesā.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

3.3. *Kādā veidā var pieprasīt informāciju un kā uz to jāatbild?*

Nav obligātas formas, informācijas pieprasījumu var veikt mutiski, rakstiski vai digitālā formātā (piemēram, pa e-pastu). Atbildi uz informācijas pieprasījumu var iesniegt jebkurā piemērotā veidā, bet jāņem vērā sekojošais:

- uz rakstisku pieprasījumu vislabāk atbildēt rakstiski. Pagātnē izplatīta metode bija tāda, ka respondents kopā ar pieteikumu iesniedza sava oficiālā identitātes dokumenta (ID) kopiju un atbildīgā persona sniedza atbildi ierakstītā vēstulē (neizmantojot piegādes aģentus). Tomēr, tā kā oficiālajā ID parasti ir lielāks datu apjoms nekā tas nepieciešams datu subjekta identificēšanai, ir ieteicams datu subjektam rakstveidā sniegt informāciju tikai par vārdu, personas kodu un/vai ID dokumenta sērijas numuru;
- pēc datu subjekta pieprasījuma, informāciju var sniegt mutiski, ja tā identitāte ir noteikta citā formā;
- ja datu subjekts pieteikumu iesniedz elektroniski (piemēram, pa e-pastu), tad informāciju sniedz plaši izmantotā elektroniskā formātā, ja vien netiek pieprasīts savādāk. Ja iespējams, pārzinis var nodrošināt attālināto piekļuvi drošai sistēmai, kas datu subjektam dod tiešu piekļuvi viņa personiskajai informācijai.

Uzmanību! Visai komunikācijai jānotiek **skaidrā un vienkāršā valodā** precīzā, pārredzamā, saprotamā un viegli pieejamā veidā (jo īpaši tas attiecas uz informāciju, kas paredzēta bērniem). Ja atbildē iekļauti saīsinājumi, pārzinim tie jāizskaidro savā atbildē.

3.4. *Vai jāpierāda pieteikuma iesniedzēja (datu subjekta) identitāte?*

Jā. Tās personas, kas pieprasa informāciju, identitātei jābūt skaidrai, jo pārzinis var pieprasīt papildu informāciju, ja viņam ir "pamatotas šaubas" par pieteikuma iesniedzēja identitāti (sk. 12.panta 6.punktu[1]).

Saskaņā ar 64.apsvērumu, pārzinim būtu jāizmanto visi saprātīgie līdzekļi, lai pārbaudītu datu subjekta, kas meklē informāciju, identitāti, jo īpaši saistībā ar tiešsaistes pakalpojumiem un tiešsaistes identifikatoriem.

Identitātes pārbaudi nepieciešams izstrādāt, lai izpildītu pienākumu nodrošināt datu drošību saskaņā ar riskiem, pretējā gadījumā varētu notikt personas datu aizsardzības pārkāpums, ja dati tiek nosūtīti nepareizam saņēmējam.

[1] Skatiet arī Souhrada-Kirchmayer, The right of access to the DSGVO, in Jahnel [Hrsg], Yearbook 17. Data Protection Law [2017] 86 f.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

Austrijas prakse saskaņā ar iepriekšējo Datu aizsardzības likumu (DSG 2000) bija tāda, ka datu subjekts kopā ar pieteikumu iesniedza identifikācijas dokumenta (oficiālā ID) kopiju, un pārzinis atbildēja ar pasta nodaļas starpniecību "personiski" ierakstītas vēstules veidā (neizmantojot piegādes aģentus). Tomēr identitāte var būt skaidra arī situācijā, piemēram, ja subjektam pastāv pastāvīgs kontakts ar informācijas sniedzēju, tādējādi tā (kā arī viņa adrese) ir zināma[2].

3.5. Maksa? Vai par informācijas sniegšanu jāatlīdzina?

Principā informācija ir jāsniedz bez maksas (sk. VDAR 12.panta 5.punktu). Tomēr attiecībā uz acīmredzami nepamatotu vai pārmērīgu pieprasījumu un jo īpaši tā regulāras atkārtošanās gadījumā, pārzinis var vai nu:

a) pieprasīt saprātīgu maksu, ņemot vērā administratīvās izmaksas, kas saistītas ar informācijas vai saziņas nodrošināšanu vai pieprasītās darbības veikšanu; vai arī

b) atteikties izpildīt pieprasījumu.

3.6. Vai datu subjektam ir pienākums iesaistīties informācijas izpaušanā?

Jā, pat ja pienākums sadarboties ir minēts tikai 63.apsvērumā, līdz šim publicētajā literatūrā galvenokārt tiek pieņemts, ka tas pastāv (tas arī tika atzīts Austrijā saskaņā ar DSG 2000): "Ja pārzinis apstrādā lielu informācijas apjomu saistībā ar datu subjektu, pārzinim būtu jāspēj pieprasīt, lai datu subjekts pirms informācijas nosūtīšanas precizētu, uz kuru informāciju un kurām apstrādes darbībām pieprasījums attiecas."[3]

3.7. Vai, sniedzot informāciju, jāņem vērā trešo personu tiesības?

Jā, saskaņā ar VDAR 15.panta 4.punktu tiesības saņemt kopiju nedrīkst nelabvēlīgi ietekmēt citu personu tiesības un brīvības. Turklāt 63.apsvērumā ir teikts, ka "minētajām tiesībām nevajadzētu nelabvēlīgi ietekmēt citu personu tiesības vai brīvības, tostarp tirdzniecības noslēpumus vai intelektuālā īpašuma tiesības un jo īpaši autortiesības, ar ko aizsargāta programmatūra. Tomēr minēto apsvērumu rezultātam nevajadzētu būt tādam, ka datu subjektam tiek atteikts sniegt jebkādu informāciju."

Tādēļ ir nepieciešams kontrolēt izpaužamos datus, parasti trešo personu personas dati (piemēram, tās personas vārds, kas apkalpo klientu un ir uzskaitīts klienta failā) ir jāsvītro no datu kopijas.

[2] Sk., piem., Austrijas Augstākās tiesas jurisprudenci: VwGH 4.7.2016, Ra 2016/04/0014; OGH 25.2.1993, 6 Ob 6/93)

[3] 63.apsvērums

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

4. Pārbaudes saraksts informācijas izpaušanai pēc pieprasījuma

Vai man ir pienākums sniegt informāciju?	Ja vietējā pašvaldība ir datu pārzinis - JĀ. Ja vietējā pašvaldība ir tikai apstrādātājs, bet saņem šādu pieprasījumu, tai nekavējoties jānosūta pieprasījums atbildīgajai personai.
Identitātes pārbaude	Personas, kas pieprasa informāciju, identitātei jābūt skaidrai. Ja šaubāties par identitāti, pieprasiet pierādījumu.
Vai informācijas izpaušana ir bez maksas?	Principā - JĀ. Ja pieprasījuma iesniedzējam vairākkārt tika sniegta viena un tā pati informācija vai pieprasījums ir nopietni traucējis pārzinim, ir iespējams paredzēt maksu. NB! Šis ir arī valsts jurisdikcijas jautājums. Tāpēc pārbaudiet jūsu darbībai piemērojamos tiesību aktus.
Vai vispār tiek apstrādāti pieprasījuma iesniedzēja personas dati?	Ja par pieprasījuma iesniedzēju nav glabāti dati vai dati jau ir izdzēsti vai dati ir neatgriezeniski anonimizēti, personas dati netiks apstrādāti un tiks sniegta tā saucamā negatīvā atbilde: "Mēs neapstrādājam nekādus personas datus par Jums".
Kādus datus un informāciju pārzinim jāsniedz?	Jāsniedz visi dati, kas tiek glabāti par attiecīgo personu. Atkarībā no sistēmu sarežģītības, tas jāņem vērā jau iepriekš (attiecībā uz apstrādes direktoriju), kurā sistēmā var atrast konkrēto kategoriju personu datus. Turklāt jānodrošina VDAR 15.panta 1. punktā minētā informācija. Ir jāievēro trešo pušu tiesības (īpaši tirdzniecības noslēpumi un to, ka trešo personu dati ir jādzēš vai jāaizklāj).

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

4.1. Informācijas nosūtīšana

Informācijas izpaušanas piemērs saskaņā ar VDAR 15.pantu

Jūsu informācijas pieprasījums

Cienījamā [vārds] kundze / godātais [vārds] kungs!

1. Atbildot uz Jūsu [datums] informācijas pieprasījumu saskaņā ar VDAR 15.pantu, ko esam saņēmuši [datums],

2. [ja atbilde tiek nosūtīta viena mēneša laikā pēc pieprasījuma saņemšanas] apstiprinām, ka mēs apstrādājam Jūsu personas datus / [ja netiek apstrādāti dati] informējam, ka Jūsu personas datu apstrāde netiek veikta.

[pagarinājuma gadījumā saskaņā ar VDAR 12.panta 3.punktu] Kā norādīts [datums] vēstulē, esam izmantojuši iespēju pagarināt termiņu līdz trim mēnešiem sakarā ar [pieprasījuma sarežģītību / Jūsu pieprasījumu skaitu / papildu skaidrojumu nepieciešamību].

3. [ja dati tiek apstrādāti] Mēs apstrādājam šādus datus par Jums: [šeit ir to faktisko datu saraksts, kas tiek apstrādāti].

Izdrukas / kopijas no attiecīgās datu apstrādes ir pieejamas pielikumā. Jebkurš datu trūkums vai to aizklāšana veikta tā, lai neietekmētu citu personu tiesības un brīvības, vai arī šī informācija neattiecas uz Jums vai Jūsu personisko informāciju.

4. [ja dati nav iegūti no datu subjekta]: Mēs esam saņēmuši Jūsu datus no [pieejamā informācija par datu izcelsmi, piemēram, valsts iestāde XY].

5. [ja piemērojams] Mēs izmantosim automatizētas lēmumu pieņemšanas / profilēšanas procedūras, kam ir juridiskas sekas vai līdzīga ietekme uz Jums: [lūdzu, aizpildiet saturīgu informāciju, kas pamato šādas darbības un to ietekmi un sekas].

6. Jums ir tiesības pieprasīt Jūsu personas datu labošanu, dzēšanu, ierobežošanu, kā arī tiesības apstrīdēt to apstrādi. Lai to izdarītu, sazinieties ar mums. Ja uzskatāt, ka Jūsu datu apstrāde ir pretrunā ar datu aizsardzības tiesību aktiem vai ja Jūsu datu aizsardzības prasības ir citādi pārkāptas, varat iesniegt sūdzību uzraudzības iestādei. Latvijā atbildīgā iestāde ir Datu valsts inspekcija.

Ar cieņu,

….

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

5. Ārējie avoti un tīmekļa vietnes

5.1. Grāmatas un publikācijas

- Souhrada-Kirchmayer, The right of access to the DSGVO, in Jahnel [Hrsg], Yearbook 17. Data Protection Law [2017] 86 f.
- *Martini in Paal/Pauly* (Ed.), Datenschutz-Grundverordnung (2016).

5.2. Citi dokumenti un prakse

- Austrijas Augstākās tiesas jurisprudence: VwGH 4.7.2016, Ra 2016/04/0014; OGH 25.2.1993, 6 Ob 6/93 Web Links
- Lai salīdzinātu izmaiņas ar Direktīvu 95/46/EK skatiet https://gdpr.report/news/2017/11/20/gdpr-subject-access-requests/

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

ProLegis

Temeiuri Juridice pentru Prelucrarea Datelor cu Caracter Personal

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

ProLegis

Cuprins

1. CADRU LEGAL 4

1.1. Carta drepturilor fundamentale a Uniunii Europene 4

1.2. Regulamentul general privind protecția datelor (RGPD) 4

2. TEMEIURI JURIDICE PENTRU PRELUCRAREA DATELOR CU CARACTER PERSONAL ÎN CADRUL RGPD 11

2.1. Consimțământul 11

2.1.1. Semnificație & cerințe legale 11

2.1.2. Aplicabilitatea la nivelul activității autorităților locale 12

2.2. Executarea / încheierea contractului cu persoana vizată 14

2.2.1. Semnificație & cerințe legale 14

2.2.2. Aplicabilitatea la nivelul activității autorităților locale 15

2.3. Obligația legală 15

2.3.1. Semnificație & cerințe legale 15

2.3.2. Aplicabilitatea la nivelul activității autorităților locale 16

2.4. Interesul vital 16

2.4.1. Semnificație & cerințe legale 16

2.4.2. Aplicabilitatea la nivelul activității autorităților locale 17

2.5. Sarcina care servește unui interes public / rezultă din exercitarea autorității publice 17

2.5.1. Semnificație & cerințe legale 17

2.5.2. Aplicabilitatea la nivelul activității autorităților locale 18

2.6. Interesele legitime 18

2.6.1. Semnificație & cerințe legale 18

2.6.2. Aplicabilitatea la nivelul activității autorităților locale 19

3. CONCLUZIE ȘI RECOMANDĂRI 20

4. BIBLIOGRAFIE 20

Cărți 20

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

Documente referitoare la Grupul de lucru "Articolul 29" 21

Link-uri Web 21

5. NOTE 21

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

1. CADRU LEGAL

1.1. Carta drepturilor fundamentale a Uniunii Europene

Articolul 8

Protecția datelor cu caracter personal

1. Orice persoană are dreptul la protecția datelor cu caracter personal care o privesc.

2. Asemenea date trebuie tratate în mod corect, în scopurile precizate și ***pe baza consimțământului persoanei interesate sau în temeiul unui alt motiv legitim prevăzut de lege****. Orice persoană are dreptul de acces la datele colectate care o privesc, precum și dreptul de a obține rectificarea acestora.*

3. Respectarea acestor norme se supune controlului unei autorități independente.

1.2. Regulamentul general privind protecția datelor (RGPD)

Considerentul (42)

[…] Pentru ca acordarea consimțământului să fie în cunoștință de cauză, persoana vizată ar trebui să fie la curent cel puțin cu identitatea operatorului și cu scopurile prelucrării pentru care sunt destinate datele cu caracter personal. Consimțământul nu ar trebui considerat ca fiind acordat în mod liber dacă persoana vizată nu dispune cu adevărat de libertatea de alegere sau nu este în măsură să refuze sau să își retragă consimțământul fără a fi prejudiciată.

Considerentul (43)

Pentru a garanta faptul că a fost acordat în mod liber, consimțământul nu ar trebui să constituie un temei juridic valabil pentru prelucrarea datelor cu caracter personal în cazul particular în care există un dezechilibru evident între persoana vizată și operator, ***în special în cazul în care operatorul este o autoritate publică****, iar acest lucru face improbabilă acordarea consimțământului în mod liber în toate circumstanțele aferente respectivei situații particulare. Consimțământul este considerat a nu fi acordat în mod liber în cazul în care aceasta nu permite să se acorde consimțământul separat pentru diferitele operațiuni de prelucrare a datelor cu caracter personal, deși acest lucru este adecvat în cazul particular, sau dacă executarea unui*

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

contract, inclusiv furnizarea unui serviciu, este condiționată de consimțământ, în ciuda faptului că consimțământul în cauză nu este necesar pentru executarea contractului.

Considerentul (44)

Prelucrarea ar trebui să fie considerată legală în cazul în care este ***necesară în cadrul unui contract sau în vederea încheierii unui contract.***

Considerentul (45)

În cazul în care prelucrarea este efectuată în conformitate cu o ***obligație legală*** *a operatorului sau în cazul în care prelucrarea este necesară pentru îndeplinirea unei sarcini care servește unui interes public sau care face parte din exercitarea autorității publice, prelucrarea ar trebui să aibă un temei în dreptul Uniunii sau în dreptul intern. Prezentul regulament nu impune existența unei legi specifice pentru fiecare prelucrare în parte. Poate fi suficientă o singură lege drept temei pentru mai multe operațiuni de prelucrare efectuate în conformitate cu o obligație legală a operatorului sau în cazul în care prelucrarea este necesară pentru îndeplinirea unei sarcini care servește unui interes public sau care face parte din exercitarea autorității publice. De asemenea, ar trebui ca scopul prelucrării să fie stabilit în dreptul Uniunii sau în dreptul intern. Mai mult decât atât, dreptul respectiv ar putea să specifice condițiile generale ale prezentului regulament care reglementează legalitatea prelucrării datelor cu caracter personal, să determine specificațiile pentru stabilirea operatorului, a tipului de date cu caracter personal care fac obiectul prelucrării, a persoanelor vizate, a entităților cărora le pot fi divulgate datele cu caracter personal, a limitărilor în funcție de scop, a perioadei de stocare și a altor măsuri pentru a garanta o prelucrare legală și echitabilă. De asemenea, ar trebui să se stabilească în dreptul Uniunii sau în dreptul intern dacă operatorul care îndeplinește o sarcină care servește unui interes public sau care face parte din exercitarea autorității publice ar trebui să fie o autoritate publică sau o altă persoană fizică sau juridică guvernată de dreptul public sau, atunci când motive de interes public justifică acest lucru, inclusiv în scopuri medicale, precum sănătatea publică și protecția socială, precum și gestionarea serviciilor de asistență medicală, de dreptul privat, cum ar fi o asociație profesională.*

Considerentul (46)

Prelucrarea datelor cu caracter personal ar trebui, de asemenea, să fie considerată legală în cazul în care este necesară în scopul asigurării protecției unui ***interes care este esențial pentru viața persoanei vizate sau pentru viața unei alte persoane fizice****. Prelucrarea datelor cu caracter personal care are drept temei interesele vitale*

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

ale unei alte persoane fizice ar trebui efectuată numai în cazul în care prelucrarea nu se poate baza în mod evident pe un alt temei juridic. Unele tipuri de prelucrare pot servi atât unor motive importante de interes public, cât și intereselor vitale ale persoanei vizate, de exemplu în cazul în care prelucrarea este necesară în scopuri umanitare, inclusiv în vederea monitorizării unei epidemii și a răspândirii acesteia sau în situații de urgențe umanitare, în special în situații de dezastre naturale sau provocate de om.

Considerentul (47)

***Interesele legitime ale unui operator, inclusiv cele ale unui operator căruia îi pot fi divulgate datele cu caracter personal sau ale unei terțe părți**, pot constitui un temei juridic pentru prelucrare, cu condiția să nu prevaleze interesele sau drepturile și libertățile fundamentale ale persoanei vizate, luând în considerare așteptările rezonabile ale persoanelor vizate bazate pe relația acestora cu operatorul. Acest interes legitim ar putea exista, de exemplu, atunci când există o relație relevantă și adecvată între persoana vizată și operator, cum ar fi cazul în care persoana vizată este un client al operatorului sau se află în serviciul acestuia. În orice caz, existența unui interes legitim ar necesita o evaluare atentă, care să stabilească inclusiv dacă o persoană vizată poate preconiza în mod rezonabil, în momentul și în contextul colectării datelor cu caracter personal, posibilitatea prelucrării în acest scop. Interesele și drepturile fundamentale ale persoanei vizate ar putea prevala în special în raport cu interesul operatorului de date atunci când datele cu caracter personal sunt prelucrate în circumstanțe în care persoanele vizate nu preconizează în mod rezonabil o prelucrare ulterioară. Întrucât legiuitorul trebuie să furnizeze temeiul juridic pentru prelucrarea datelor cu caracter personal de către autoritățile publice, temeiul juridic respectiv nu ar trebui să se aplice prelucrării de către autoritățile publice în îndeplinirea sarcinilor care le revin. Prelucrarea de date cu caracter personal strict necesară în scopul prevenirii fraudelor constituie, de asemenea, un interes legitim al operatorului de date în cauză. Prelucrarea de date cu caracter personal care are drept scop marketingul direct poate fi considerată ca fiind desfășurată pentru un interes legitim.*

Considerentul (48)

Operatorii care fac parte dintr-un grup de întreprinderi sau instituții afiliate unui organism central pot avea un interes legitim de a transmite date cu caracter personal în cadrul grupului de întreprinderi în scopuri administrative interne, inclusiv în scopul prelucrării datelor cu caracter personal ale clienților sau angajaților. Principiile

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

generale ale transferului de date cu caracter personal, în cadrul unui grup de întreprinderi, către o întreprindere situată într-o țară terță rămân neschimbate.

Considerentul (49)

Prelucrarea datelor cu caracter personal în măsura strict necesară și proporțională în scopul asigurării securității rețelelor și a informațiilor, și anume capacitatea unei rețele sau a unui sistem de informații de a face față, la un anumit nivel de încredere, evenimentelor accidentale sau acțiunilor ilegale sau rău intenționate care compromit disponibilitatea, autenticitatea, integritatea și confidențialitatea datelor cu caracter personal stocate sau transmise, precum și securitatea serviciilor conexe oferite de aceste rețele și sisteme, sau accesibile prin intermediul acestora, de către autoritățile publice, echipele de intervenție în caz de urgență informatică, echipele de intervenție în cazul producerii unor incidente care afectează securitatea informatică, furnizorii de rețele și servicii de comunicații electronice, precum și de către furnizorii de servicii și tehnologii de securitate, constituie un interes legitim al operatorului de date în cauză. Acesta ar putea include, de exemplu, prevenirea accesului neautorizat la rețelele de comunicații electronice și a difuzării de coduri dăunătoare și oprirea atacurilor de „blocare a serviciului", precum și prevenirea daunelor aduse calculatoarelor și sistemelor de comunicații electronice.

Considerentul (50)

Prelucrarea datelor cu caracter personal în alte scopuri decât scopurile pentru care datele cu caracter personal au fost inițial colectate ar trebui să fie permisă doar atunci când prelucrarea este compatibilă cu scopurile respective pentru care datele cu caracter personal au fost inițial colectate. În acest caz nu este necesar un temei juridic separat de cel pe baza căruia a fost permisă colectarea datelor cu caracter personal. În cazul în care prelucrarea este necesară pentru îndeplinirea unei sarcini care servește unui interes public sau care rezultă din exercitarea autorității publice cu care este învestit operatorul, dreptul Uniunii sau dreptul intern poate stabili și specifica sarcinile și scopurile pentru care prelucrarea ulterioară ar trebui considerată a fi compatibilă și legală. Prelucrarea ulterioară în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice ar trebui considerată ca reprezentând operațiuni de prelucrare legale compatibile. Temeiul juridic prevăzut în dreptul Uniunii sau în dreptul intern pentru prelucrarea datelor cu caracter personal poate constitui, de asemenea, un temei juridic pentru prelucrarea ulterioară. Pentru a stabili dacă scopul prelucrării ulterioare este compatibil cu scopul pentru care au fost colectate inițial datele cu caracter personal, operatorul, după ce a îndeplinit toate

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

cerințele privind legalitatea prelucrării inițiale, ar trebui să țină seama, printre altele, de orice legătură între respectivele scopuri și scopurile prelucrării ulterioare preconizate, de contextul în care au fost colectate datele cu caracter personal, în special de așteptările rezonabile ale persoanelor vizate, bazate pe relația lor cu operatorul, în ceea ce privește utilizarea ulterioară a datelor, de natura datelor cu caracter personal, de consecințele prelucrării ulterioare preconizate asupra persoanelor vizate, precum și de existența garanțiilor corespunzătoare atât în cadrul operațiunilor de prelucrare inițiale, cât și în cadrul operațiunilor de prelucrare ulterioare preconizate.

În cazul în care persoana vizată și-a dat consimțământul sau prelucrarea se bazează pe dreptul Uniunii sau pe dreptul intern, care constituie o măsură necesară și proporțională într-o societate democratică pentru a proteja, în special, obiective importante de interes public general, operatorul ar trebui să aibă posibilitatea de a prelucra în continuare datele cu caracter personal, indiferent de compatibilitatea scopurilor. În orice caz, aplicarea principiilor stabilite de prezentul regulament și, în special, informarea persoanei vizate cu privire la aceste alte scopuri și la drepturile sale, inclusiv dreptul la opoziție, ar trebui să fie garantate. Indicarea unor posibile infracțiuni sau amenințări la adresa siguranței publice de către operator și transmiterea către o autoritate competentă a datelor cu caracter personal relevante în cazuri individuale sau în mai multe cazuri legate de aceeași infracțiune sau de aceleași amenințări la adresa siguranței publice ar trebui considerată ca fiind în interesul legitim urmărit de operator. Cu toate acestea, o astfel de transmitere în interesul legitim al operatorului sau prelucrarea ulterioară a datelor cu caracter personal ar trebui interzisă în cazul în care prelucrarea nu este compatibilă cu o obligație legală, profesională sau cu o altă obligație de păstrare a confidențialității.

Articolul 4

Definiții

În sensul prezentului regulament:

[…]

(11) „consimțământ” al persoanei vizate înseamnă orice ***manifestare de voință liberă, specifică, informată și lipsită de ambiguitate a persoanei vizate prin care aceasta acceptă, printr-o declarație sau printr-o acțiune fără echivoc, ca datele cu caracter personal care o privesc să fie prelucrate****;*

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

Articolul 6

Legalitatea prelucrării

*1. Prelucrarea este legală numai dacă și în măsura în care se aplică **cel puțin una dintre următoarele condiții:***

(a) persoana vizată și-a dat consimțământul pentru prelucrarea datelor sale cu caracter personal pentru unul sau mai multe scopuri specifice;

(b) prelucrarea este necesară pentru executarea unui contract la care persoana vizată este parte sau pentru a face demersuri la cererea persoanei vizate înainte de încheierea unui contract;

(c) prelucrarea este necesară în vederea îndeplinirii unei obligații legale care îi revine operatorului;

(d) prelucrarea este necesară pentru a proteja interesele vitale ale persoanei vizate sau ale altei persoane fizice;

(e) prelucrarea este necesară pentru îndeplinirea unei sarcini care servește unui interes public sau care rezultă din exercitarea autorității publice cu care este învestit operatorul;

(f) prelucrarea este necesară în scopul intereselor legitime urmărite de operator sau de o parte terță, cu excepția cazului în care prevalează interesele sau drepturile și libertățile fundamentale ale persoanei vizate, care necesită protejarea datelor cu caracter personal, în special atunci când persoana vizată este un copil.

Litera (f) din primul paragraf nu se aplică în cazul prelucrării efectuate de autorități publice în îndeplinirea atribuțiilor lor.

2. Statele membre pot menține sau introduce dispoziții mai specifice de adaptare a aplicării normelor prezentului regulament în ceea ce privește prelucrarea în vederea respectării alineatului (1) literele (c) și (e) prin definirea unor cerințe specifice mai precise cu privire la prelucrare și a altor măsuri de asigurare a unei prelucrări legale și echitabile, inclusiv pentru alte situații concrete de prelucrare, astfel cum este prevăzut în capitolul IX.

3. Temeiul pentru prelucrarea menționată la alineatul (1) literele (c) și (e) trebuie să fie prevăzut în:

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

(a) dreptul Uniunii; sau

(b) dreptul intern care se aplică operatorului.

Scopul prelucrării este stabilit pe baza respectivului temei juridic sau, în ceea ce privește prelucrarea menționată la alineatul (1) litera (e), este necesar pentru îndeplinirea unei sarcini efectuate în interes public sau în cadrul exercitării unei funcții publice atribuite operatorului. Respectivul temei juridic poate conține dispoziții specifice privind adaptarea aplicării normelor prezentului regulament, printre altele: condițiile generale care reglementează legalitatea prelucrării de către operator; tipurile de date care fac obiectul prelucrării; persoanele vizate; entitățile cărora le pot fi divulgate datele și scopul pentru care respectivele date cu caracter personal pot fi divulgate; limitările legate de scop; perioadele de stocare; operațiunile și procedurile de prelucrare, inclusiv măsurile de asigurare a unei prelucrări legale și echitabile cum sunt cele pentru alte situații concrete de prelucrare astfel cum sunt prevăzute în capitolul IX. Dreptul Uniunii sau dreptul intern urmărește un obiectiv de interes public și este proporțional cu obiectivul legitim urmărit.

4. În cazul în care prelucrarea în alt scop decât cel pentru care datele cu caracter personal au fost colectate nu se bazează pe consimțământul persoanei vizate sau pe dreptul Uniunii sau dreptul intern, care constituie o măsură necesară și proporțională într-o societate democratică pentru a proteja obiectivele menționate la articolul 23 alineatul (1), operatorul, pentru a stabili dacă prelucrarea în alt scop este compatibilă cu scopul pentru care datele cu caracter personal au fost colectate inițial, ia în considerare, printre altele:

(a) orice legătură dintre scopurile în care datele cu caracter personal au fost colectate și scopurile prelucrării ulterioare preconizate;

(b) contextul în care datele cu caracter personal au fost colectate, în special în ceea ce privește relația dintre persoanele vizate și operator;

(c) natura datelor cu caracter personal, în special în cazul prelucrării unor categorii speciale de date cu caracter personal, în conformitate cu articolul 9, sau în cazul în care sunt prelucrate date cu caracter personal referitoare la condamnări penale și infracțiuni, în conformitate cu articolul 10;

(d) posibilele consecințe asupra persoanelor vizate ale prelucrării ulterioare preconizate;

(e) existența unor garanții adecvate, care pot include criptarea sau pseudonimizarea.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

2. TEMEIURI JURIDICE PENTRU PRELUCRAREA DATELOR CU CARACTER PERSONAL ÎN CADRUL RGPD

2.1. Consimțământul

2.1.1. Semnificație & cerințe legale

Consimțământul este unul dintre cele șase temeiuri juridice menționate în articolul 6 al RGPD. Conform acestui document, pentru a fi valabil, consimțământul trebuie să constituie o manifestare de voință liberă, specifică, în cunoștință de cauză și lipsită de ambiguitate.

- **'voință liberă'** = implică alegere și control veritabile din partea persoanelor vizate[i]. Dacă apar consecințe nefavorabile pentru persoana vizată, în cazul în care nu este de acord cu prelucrarea datelor / își retrage consimțământul deja acordat (de exemplu, refuzarea serviciului, costurile ridicate ale bunurilor / serviciilor – taxe, prețuri etc.), consimțământul trebuie considerat că nu este acordat în mod liber. Din cauza dezechilibrului de putere dintre autoritățile publice și persoanele vizate, consimțământul se dovedește a fi rareori un instrument util de prelucrare a datelor atunci când este aplicat de către oficialități;
- **'voință specifică'** = în strânsă legătură cu cerința conform căreia persoana vizată consimte pentru unul sau mai multe scopuri specifice ale prelucrării (așa-numita „granularitate" („detaliere" / „distingere a scopurilor") a consimțământului[ii]) și cu principiul specificării scopului. Fiecare scop al prelucrării datelor trebuie să i se definească persoanei vizate în mod clar, de la bun început. Persoana vizată ar trebui să poată alege scopul pentru care consimte (de exemplu, consmite pentru scopurile A, B și C, însă nu pentru D și E). Informațiile cu privire la consimțământ ar trebui să fie clar separate de informațiile referitoare la alte chestiuni. Pentru orice nou scop de prelucrare trebuie obținut un nou consimțământ, iar operatorii trebuie să furnizeze informații specifice de fiecare dată, în funcție de scopul vizat;
- **'în cunoștință de cauză'** = cerințele minime din RGPD includ furnizarea de informații cu privire la operatorul de date și scopurile prelucrării. Grupul de lucru "Articolul 29" recomandă includerea unor informații suplimentare: tipul de date colectate și utilizate; dreptul de retragere a consimțământului; informații referitoare la utilizarea datelor pentru decizii bazate strict pe prelucrarea automatizată, inclusiv crearea de profiluri[iii]; în cazul transferurilor – informații despre posibilele riscuri ale transferurilor de date către o țară terță, în absența unei decizii privind caracterul adecvat și a unor măsuri de siguranță corespunzătoare[iv].
- **'voință lipsită de ambiguitate'** = consimțământul trebuie să fie acordat de către persoana vizată printr-o declarație sau printr-o acțiune fără echivoc.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

Consimțământul trebuie să fie întotdeauna dat printr-o acțiune verbală sau scrisă. În acest sens, potrivit RGPD, absența unui răspuns, căsuțele bifate în prealabil sau lipsa unei acțiuni nu pot constitui un consimțământ valabil;

- **După cum poate fi acordat, poate fi și retras** = consimțământul poate fi retras în orice moment. Acest lucru nu este necesar să se întâmple în cadrul aceleiași acțiuni, însă procesul de retragere ar trebui să fie la fel de simplu ca și procesul de acordare a consimțământului (de exemplu, bifarea unei căsuțe într-o declarație online pentru a consimți primirea ziarului municipalității este tot atât de ușoară ca și click-ul pe un link din corpul e-mailului cu newsletter, care face posibilă dezabonarea și, odată cu aceasta, retragerea consimțământului);
- **Cerințe specifice cu privire la consimțământul copiilor** = RGPD tratează copiii drept o categorie vulnerabilă a persoanelor vizate. Astfel, ei merită o protecție specială, deoarece pot fi mai puțin conștienți de riscurile, consecințele, măsurile de siguranță în cauză și drepturile lor în ceea ce privește prelucrarea datelor cu caracter personal. În cazul oferirii de servicii ale societății informaționale unui copil (de exemplu, campanii educaționale online realizate pe site-urile municipalităților, care necesită colectarea datelor cu caracter personal ale copiilor), consimțământul pentru prelucrarea datelor copiilor sub 16 ani (statele membre pot reduce această vârstă până la 13 ani) trebuie să fie acordat sau autorizat de titularul răspunderii părintești asupra copilului;
- **Consimțământul conform directivei 95/46** = consimțământul obținut în cadrul vechiului regim nu trebuie neapărat să fie revizuit. În cazul în care consimțământul corespunde cerințelor stabilite în RGPD, chiar dacă a fost obținut în baza directivei, ar trebui să fie considerat în continuare valabil pentru prelucrare.

Obținerea adecvată a consimțământului, însoțită de dovezi, cade în sarcina operatorului de date [v].

2.1.2. Aplicabilitatea la nivelul activității autorităților locale

În practică, consimțământul constituie rareori un temei juridic fundamental în baza căruia autoritățile locale (AL) să poată prelucra în mod legitim datele cu caracter personal ale cetățenilor. Această concluzie decurge din cerințele RGPD pe care consimțământul trebuie să le îndeplinească pentru a fi valabil.

În primul rând, „acordarea în mod liber", altfel spus inexistența unor consecințe negative pentru persoana vizată în cazul în care aceasta nu consimte, înseamnă că în orice situație în care AL își exercită atribuțiile, cosimțământul nu poate fi utilizat ca temei juridic valabil pentru prelucrarea datelor. Controlul în scopul îndeplinirii corespunzătoare a obligațiilor publice ale cetățenilor (de exemplu, colectarea taxelor și impozitelor locale, înregistrarea achiziționării de imobile / vehicule etc.), precum și impunerea de sancțiuni în cazul

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

nerespectării acestor obligații sunt în mod inerent legate de dreptul (și obligația) AL de a-și exercita puterea de constrângere. Din acest motiv persoanele vizate nu au propriu-zis libertatea de a consimți sau de a nu consimți în scopul prelucrării datelor lor personale. Ele se află, de fapt, într-un raport de subordoanre și sunt obligate prin lege să coopereze cu AL.

În al doilea rând, consimțământul poate fi retras „în orice moment". În cazul în care consimțământul a constituit temeiul legitim pentru prelucrarea datelor cu caracter personal, iar cetățenii respectă la modul general legile, în principiu, orice cetățean care acționează cu rea-credință (de exemplu, nu este dispus să îndeplinească anumite obligații publice) își poate retrage oricând consimțământul și se poate folosi de această retragere pentru a crea obstacole, practic, pentru „a bloca" funcționarea normală a AL. În cazul retragerii consimțământului, AL, în calitate de operator de date, ar trebui să înceteze prelucrarea. Acest lucru este însă de neconceput, deoarece ar conduce la subminarea ideii de exercitare a puterii publice.

Prin urmare, în situațiile descrise mai sus, consimțământul nu este instrumentul potrivit pentru prelucrarea datelor.

Potrivit WP29, *„utilizarea consimțământului ca bază legală pentru prelucrarea datelor de către autoritățile publice* ***nu este în totalitate exclusă*** *în cadrul juridic al RGPD"*[vi]. Astfel, consimțământul ar putea fi un instrument util în situațiile în care AL nu își exercită funcțiile sale obișnuite sau atunci când prelucrarea datelor are un caracter facultativ, existând proceduri de prelucrare implicită pentru cazurile în care persoana vizată nu consimte. Iată câteva exemple:

- AL și autoritățile guvernamentale au nevoie de aceleași informații cu privire la un cetățean pentru emiterea unui act juridic, dar nu își pot accesa reciproc bazele de date. Întrucât ambele solicită aceleași informații, ar putea să ceară consimțământul cetățeanului pentru combinarea datelor de care dispune fiecare, astfel încât să fie evitată dublarea procedurilor și a corespondenței. Ambele instituții ar trebui să garanteze că acest lucru este facultativ și că documentul poate fi eliberat chiar dacă cetățeanul nu acceptă varianta propusă[vii];
- AL îi poate notifica prin e-mail pe cetățenii care participă la acțiuni administrative. Aceasta se petrece în regim „opt-in", cu alte cuvinte, cetățenii sunt liberi să opteze pentru notificare (prin bifarea unei căsuțe dintr-un formular în format fizic sau electronic și furnizarea adresei de e-mail). În cazul refuzului de a consimți / retragerii consimțământului, AL ar trebui să dispună de o procedură implicită de

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

notificare (de exemplu, scrisoare recomandată). Prelucrarea adresei de e-mail în acest caz are la bază consimțământul;

- AL poate pune la dispoziția cetățenilor opțiunea de a se abona pentru primirea de invitații la evenimente organizate de aceasta (expoziții muzeale, premiere la teatru, campanii de colectare a gunoiului, campanii / competiții educaționale în școli ș.a.) Abonamentul necesită furnizarea datelor de contact (adresă poștală, număr de telefon, e-mail etc.), precum și date despre preferințele personale (hobby-uri, interese ș.a.m.d.). Prelucrarea acestor date se bazează pe consimțământ, deoarece cetățenii au dreptul de a renunța la astfel de notificări în mod liber, în orice moment, fără a li se aduce prejudicii.

2.2. *Executarea / încheierea contractului cu persoana vizată*

2.2.1. *Semnificație & cerințe legale*

În Articolul 6, alineatul (1), punctul (b) din RGPD sunt introduse două temeiuri juridice **distincte** pentru prelucrarea datelor cu caracter personal:

(i) situațiile în care prelucrarea este necesară pentru executarea unui contract la care persoana vizată este parte;

(ii) situațiile în care prelucrarea are loc *înainte de* încheierea unui contract. Sunt avute în vedere relațiile precontractuale, cu condiția ca demersurile să fie făcute la cererea persoanei vizate, nu din inițiativa operatorului sau a unei terțe părți[viii].

Primul aspect ar trebui interpretat în sens strict, fără a include situațiile în care prelucrarea nu se impune cu adevărat executării unui contract, ci mai curând pe cele în care este aplicată unilateral de către operator asupra persoanei vizate[ix]. În conformitate cu interpretarea oferită de WP29 aceluiași temei, aflat însă sub incidența vechii directive 95/46, acesta se aplică numai la ceea ce este necesar pentru **executarea** unui contract. Cu alte cuvinte, dacă prelucrarea acoperă executarea obișnuită a unui contract, ea poate intra sub incidența temeiului juridic menționat. Acest temei ar fi valabil pentru situațiile în care prelucrarea are loc în cadrul unui contract, indiferent de etapa de contractare[x]. Cu toate acestea, orice alte acțiuni generate de neconformități sau incidente care conduc la anularea executării contractului nu intră în domeniul de aplicare al acestui temei juridic. Astfel de tipuri de prelucrare ar presupune aplicarea unor temeiuri diferite – de pildă, prevalarea intereselor legitime ale operatorului de date.

Al doilea aspect poate include prelucrarea necesară pregătirii ofertelor, recrutării de personal etc. Totuși, verificările în detaliu ale candidaților ar lua timp și, de aceea, nu ar fi justificate ca măsuri solicitate de persoana vizată.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

În general, acest temei juridic este interpretat în sens restrictiv de către autoritățile de reglementare, astfel încât să le permită operatorilor să demonstreze că fără prelucrare contractul nu poate să fie finalizat[xi].

2.2.2. Aplicabilitatea la nivelul activității autorităților locale

Acest temei juridic pentru prelucrarea datelor cu caracter personal poate fi aplicat de către AL cel puțin în următoarele domenii:

- Prelucrarea datelor angajaților – de exemplu, prelucrarea informațiilor salariale și a detaliilor contului bancar, care permit plătirea salariilor[xii];
- Prelucrarea datelor privind încheierea contractelor de achiziții publice – acest temei juridic contractual se poate suprapune cu un alt temei pentru prelucrarea datelor cu caracter personal – cum ar fi obligația legală a AL de prelucrare a datelor în cadrul procedurilor administrației publice impuse de lege;
- Prelucrarea în contextul relațiilor dintre, pe de o parte, anumite entități private deținute integral sau parțial de municipalitate / stat și, pe de altă parte, cetățeni – de exemplu, instituții care asigură, în urma încheierii de contracte, servicii de transport în comun la oraș / sat, servicii de utilități (electricitate, gaz, apă etc.).

2.3. Obligația legală

2.3.1. Semnificație & cerințe legale

Acest temei juridic necesită o dispoziție clară introdusă fie la nivel legislativ, fie la nivel sub-legislativ (legislație secundară, cum este numită în unele state membre), care obligă operatorul să efectueze prelucrarea. WP29 evidențiază faptul că legea trebuie să îndeplinească toate condițiile relevante pentru validarea obligației și, de asemenea, să respecte legea prind protecția datelor, inclusiv cerința necesității, proporționalității și limitării scopului[xiii]. RGPD prevede explicit că obligația legală trebuie să fie cumulativ:

(i) o obligație la nivelul legislației UE sau a statelor membre, căreia i se supune operatorul. WP29 a oferit deja următoarea interpretare în conformitate cu vechea directivă 95/46: obligațiile care decurg din legislația țărilor terțe (cum ar fi, obligația de a stabili scheme de avertizare împotriva corupției în temeiul legii Sarbanes–Oxley din 2002, din Statele Unite) nu cad sub incidența obligației legale de bază. Pentru a fi valabilă, o obligație legală a unei țări terțe ar trebui să fie recunoscută și integrată oficial în ordinea juridică a statului membru în cauză – de exemplu, sub forma unui acord internațional;

(ii) „clară și precisă", iar aplicarea sa este previzibilă pentru cei care trebuie să o respecte. Considerentele 41 și 45 din RGPD arată clar că obligația legală care face obiectul discuției nu trebuie să fie statutară, ceea ce ar putea avea consecințe practice pentru țările cu drept comun – e suficient dacă satisface

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

criteriul „clarității și preciziei”. O obligație legală poate acoperi mai multe operațiuni de prelucrare, astfel încât să nu fie necesară identificarea unei obligații pentru fiecare dintre acestea în parte[xiv].

WP29 a indicat că aplicarea acestui temei juridic nu este la latitudinea operatorului, cu alte cuvinte acesta nu are de ales dacă să îndeplinească sau nu obligația. Angajamentele unilateral dobândite și parteneriatele publicat-private nu intră sub incidența acestui temei juridic[xv]. Obligația legală privită ca temei pentru prelucrarea datelor cu caracter personal ar trebui să se aplice în baza dispozițiilor care se referă în mod explicit la natura și scopul prelucrării. Operatorul nu ar trebui să dea dovadă de o discreție exagerată în modul de respectare a obligației legale[xvi].

WP29 recunoaște în mod explicit că, în anumite cazuri, legislația poate stabili doar un obiectiv general, în timp ce la un alt nivel sunt impuse obligații cu caracter mai specific (de exemplu, prin intermediul legislației secundare sau al unei decizii emise de autoritatea publică). Potrivit WP29, acest lucru poate conduce și la obligații legale, cu condiția ca natura și scopul prelucrării să fie bine conturate și să facă obiectul unui temei juridic adecvat[xvii].

2.3.2. Aplicabilitatea la nivelul activității autorităților locale

În practică, obligația legală reprezintă unul dintre cele mai importante temeiuri juridice exercitate de AL în scopul prelucrării datelor cu caracter personal. Acest temei vizează atât situațiile legate de furnizarea serviciilor administrative / facilitarea îndeplinirii obligațiilor publice ale cetățenilor, cât și îndeplinirea anumitor obligații specifice de către AL, în calitatea lor de angajatori. Temeiul poate fi aplicat, de exemplu, în următoarele situații:

- colectarea de date de către AL în scopul soluționării penalităților pentru parcări în locații neautorizate;
- raportarea datelor salariale ale angajaților AL către autoritățile fiscale sau de securitate socială[xviii].

2.4. Interesul vital

2.4.1. Semnificație & cerințe legale

Acest temei juridic trebuie interpretat în sens strict. WP29 reafirmă că interesul vital trebuie să aibă o aplicare limitată[xix]. Noțiunea de „interes vital” este corelată cu amenințarea iminentă a bunurilor fundamentale ale persoanei vizate (viața, sănătatea, integritatea corporală etc.). În teoria generală a dreptului se recomandă ca prelucrarea să fie vitală pentru supraviețuirea individului[xx]. Conform interpretării oferite de WP29 vechii directive 95/46, amenințarea ar trebui să fie **imediată**, altfel spus colectarea și prelucrarea datelor cu caracter personal la scară largă în scopuri pur preventive nu poate

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

face parte din domeniul de aplicare al acestui temei juridic[xxi]. Considerentul 46 din RGPD autorizează în mod explicit prelucrarea în scopuri umanitare, inclusiv pentru monitorizarea epidemiilor și a răspândirii acestora, sau în situații de urgență precum dezastrele naturale sau cele provocate de om (în asemenea scenarii interesul vital se poate suprapune cu cel public). În acest sens, interpretarea strictă impusă în momentul de față de WP29 ar putea deveni mai permisivă pe viitor.

Totodată, trebuie remarcat faptul că, în conformitate cu vechea directivă 95/46, temeiul interesului vital făcea referire numai la persoana vizată. Odată cu RGPD, domeniul de aplicare al acestui temei juridic se lărgește – include nu numai persoana vizată, ci și o altă persoană fizică. RGPD prevede în mod expres că prelucrarea datelor cu caracter personal care are drept temei interesul vital al unei alte persoane fizice ar trebui efectuată numai în cazul în care prelucrarea nu se poate baza **în mod evident** pe un alt temei juridic. Cu alte cuvinte, fundamentarea prelucrării pe interes vital ar fi mai degrabă o soluție „de ultim moment" pentru operatori.

2.4.2. Aplicabilitatea la nivelul activității autorităților locale

Posibilitatea aplicării acestui temei de către AL este destul de limitată. Din punct de vedere teoretic, interesul vital poate fi invocat într-un număr redus de cazuri – de exemplu, pentru a justifica prelucrarea datelor personale ale angajaților sau cetățenilor în situații de urgență care s-au petrecut în jurisdicția AL și dacă nu există alt temei pentru o asemenea prelucrare (bunăoară, obligația legală sau exercitatrea autorității publice).

2.5. Sarcina care servește unui interes public / rezultă din exercitarea autorității publice

2.5.1. Semnificație & cerințe legale

Sarcina sau autoritatea operatorului de date ar trebui stabilite de legislația UE sau a statului membru din care face parte acesta. Potrivit vechii directive 95/46, îndeplinirea unor sarcini care servesc interesului public al unei țări terțe sau care fac parte din exercitarea unei autorități publice ce se supune unei legislații străine nu intră în domeniul de aplicare al acestei dispoziții[xxii]. RGPD continuă această abordare.

Analogul acestei dispoziții din vechea directivă a fost folosit pentru a acoperi două situații diferite:

(i) operatorul este o autoritate publică sau are o sarcină de interes public (dar nu este neapărat obligat să prelucreze date), iar prelucrarea este necesară pentru exercitarea autorității sau pentru îndeplinirea sarcinii, sau

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

(ii) operatorul nu este o autoritate publică, însă i se solicită să divulge date de către o terță parte care deține această calitate[xxiii].

RGPD a eliminat al doilea criteriu – nu mai sunt relevante pentru justificarea prelucrării situațiile în care exercitarea autorității publice este atribuită unei părți căreia îi sunt divulgate date[xxiv]. Cu alte cuvinte, circumstanțele în care un operator se poate baza pe acest temei juridic sunt mai restrânse decât înainte.

În mod obișnuit, sarcinile care servesc unui interes public sau care rezultă din exercitarea autorității publice ar trebui atribuite prin legi statutare sau alte reglementări de ordin juridic. WP29 a admis în mod explicit că, după introducerea RGPD, acest temei juridic trebuie interpretat astfel încât să permită autorităților publice un anumit grad de flexibilitate care să le asigure buna gestionare și funcționare. În acest sens, asemenea activități nu ar trebui să se încadreze în domeniul de aplicare al acestui temei juridic, prelucrarea datelor cu caracter personal putând fi justificată prin temeiul intereselor legitime[xxv].

Nu în ultimul rând, trebuie remarcat faptul că persoanele vizate au dreptul să se opună prelucrării care se bazează pe acest temei. Este responsabilitatea operatorului să demonstreze că are motive legitime convingătoare pentru prelucrarea datelor cu caracter personal[xxvi].

2.5.2. Aplicabilitatea la nivelul activității autorităților locale

În conformitate cu Articolul 6, alineatul (1), punctul (e) din RGPD, sarcina care servește unui interes public sau care rezultă din exercitarea autorității publice reprezintă cel mai important temei legal pentru activitățile AL. Din exemplele oferite de WP29 pentru ilustrarea aplicării acestui temei fac parte:

- o autoritate fiscală care colectează și prelucrează declarația fiscală a unei persoane pentru a stabili și verifica valoarea impozitului care trebuie plătit – în mod analog, acest temei poate fi aplicat și de către autoriățile care administrează impozitele locale;
- un organism guvernamental local (o primărie) responsabilă de administrarea unei biblioteci, a unei școli sau piscine.

2.6. Interesele legitime

2.6.1. Semnificație & cerințe legale

Temeiul legal al intereselor legitime cuprinde două elemente:

(i) Interesele legitime ale unui operator / unei terțe părți:

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

a. Conceptul de „interes” este definit de WP29 ca o miză mai largă pe care o poate avea un operator în prelucrarea datelor sau ca un beneficiu pe care operatorul îl obține – sau pe care societatea îl poate obține – în urma prelucrării[xxvii]. Interesul poate fi benefic pentru societatea în ansamblu sau numai pentru operator / partea terță;
b. Conceptul de „legitimitate” este în mod inerent legat de respectarea legii – atât legislația cu privire la protecția datelor, cât și cea care vizează activitatea operatorului. Cu alte cuvinte, orice scopuri ilegale urmărite de operator / partea terță ar descalifica aplicabilitatea acestui temei juridic. WP29 a făcut o enumerare neexhaustivă a celor mai frecvente situații în care ar putea fi aplicat interesul legitim în conformitate cu vechea directivă 95/46. Domeniile variază de la publicitate / scopuri de atragere a atenției (marketing, reclame, mesaje necomerciale nesolicitate, inclusiv campanii politice sau strângeri de fonduri caritabile) la activități de interes social general (avertismente, exercitarea dreptului la libertatea de exprimare sau informare, prevenirea fraudei, semnalarea abuzurilor în serviciu sau a spălării banilor).

(ii) Interesele legitime ar trebui să prevaleze asupra intereselor, drepturilor și libertăților fundamentale ale persoanei vizate – ar trebui aplicat de la caz la caz un test de echilibrare. Această cerință este în mod inerent legată de principiul proporționalității. Deși operatorul de date / partea terță ar putea avea interese legimite ca să efectueze prelucrarea, se poate întâmpla ca aceasta să fie disproporționată (de exemplu, este prea intruzivă, la o scară prea mare, fără limitări și garanții corespunzătoare etc.). Într-o astfel de situație, prelucrarea nu ar fi justificată. WP29 menționează că pentru realizarea testui de echilibrare ar trebui luați în considerare următorii factori:

a. evaluarea intereselor legitime ale operatorului;
b. impactul asupra persoanelor vizate;
c. un echilibru porvizoriu și
d. măsuri suplimentare de siguranță aplicate de operator pentru a preveni orice impact nefavorabil asupra persoanelor vizate[xxviii].

2.6.2. Aplicabilitatea la nivelul activității autorităților locale

RGPD limitează în mod considerabil aplicabilitatea temeiului intereselor legitime la nivelul autorităților publice. RGPD prevede explicit că acest temei nu se aplică prelucrării efectuate de autoritățile publice în îndeplinirea sarcinilor proprii. Motivul este că legea le investește cu îndeplinirea sarcinilor.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

Prin urmare, este recomandabil ca AL, care se bazează pe interese legitime pentru a-și îndeplini propriile sarcini, să ia în considerare ce alt temei juridic ar putea să aplice pentru prelucrarea datelor cu caracter personal (de exemplu, sarcina care servește unui interes public sau care rezultă din exercitarea autorității publice).

Cu toate acestea, temeiul intereselor legitime poate fi aplicat de către AL în cadrul proceselor interne – bunăoară, în activitățile de resurse umane.

3. CONCLUZIE ȘI RECOMANDĂRI

Capacitatea de a determina ce temeiuri juridice pot fi aplicate în funcție de scopul prelucrării este esențială pentru orice operator de date, având în vedere că este responsabil să asigure legalitatea prelucrării. Mai mult decât atât, informația referitoare la tipurile de temeiuri și tipurile de scopuri existente pentru prelucrarea datelor reprezintă unul dintre elementele-cheie ale principiului transparenței, fiind inclusă printre informațiile pe care operatorul trebuie să le pună la dispoziția fiecărei persoane vizate (articolele 13 și 14 ale RGPD). În consecință, atât operatorii de date publice, cât și cei privați trebuie să cunoască semnificația fiecărui temei juridic menționat în articolul 6 al RGPD. Regulamentul nu prevede noi temeiuri, ci modifică cerințele și condițiile de aplicabilitate pentru unele dintre ele (de exemplu, consimțământul, interesele legitime). În orice caz, identificarea unui temei juridic corect reprezintă un prim pas în direcția asigurării respectării standardelor RGPD în cadrul organizației. În teorie, se recomandă ca un operator prudent să își ia toate măsurile pentru a se asigura că, dacă autoritățile de supraveghere îi solicită dovezi, el poate să indice criteriile care au stat la baza prelucrării și a notificării corespunzătoare a persoanelor vizate[xxix].

4. BIBLIOGRAFIE

Cărți

- **Voigt, P., von dem Bussche, A.** – The EU General Data Protection Regulation (GDPR) – A Practical Guide, Springer International Publishing (2017);
- **Boardman, R., Mullock, J., Mole, A.** – Bird & Bird Guide to General Data Protection Regulation (2016);
- **EU** General Data Protection Regulation (GDPR). An Implementation and Compliance Guide, IT Governance Publishing, Cambridgeshire (2016);
- **European** Data Protection. Law and Practice, Executive Editor: Edurado Ustaran, CIPP/E, Partner, Hogan Lovells, IAPP (2018);

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

Documente referitoare la Grupul de lucru "Articolul 29"

- WP29, Guidelines on Consent under Regulation 2016/679, WP 259;
- WP29, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, WP 217;

Link-uri Web

- http://europa.eu/rapid/press-release_IP-18-386_en.htm
- https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en
- https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/grounds-processing/when-can-personal-data-be-processed_en
- https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/grounds-processing/what-does-grounds-legitimate-interest-mean_en
- https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/grounds-processing/when-consent-valid_en
- https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/grounds-processing/does-consent-given-25-may-2018-continue-be-valid-once-gdpr-starts-apply-25-may-2018_en
- https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/grounds-processing/what-if-somebody-withdraws-their-consent_en
- https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/grounds-processing/what-if-somebody-withdraws-their-consent_en

5. NOTE

[i] WP29, Guidelines on Consent under Regulation 2016/679, WP 259, p. 6.
[ii] WP29, Guidelines on Consent under Regulation 2016/679, WP 259, p. 11-12.
[iii] Mai multe informații referitoare la profiluri se regăsesc în WP29 Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (proiect).
[iv] WP29, Guidelines on Consent under Regulation 2016/679, WP 259, p. 13.
[v] EU General Data Protection Regulation (GDPR). An Implementation and Compliance Guide, IT Governance Publishing, Cambridgeshire (2016), p. 189-190.
[vi] WP29, Guidelines on Consent under Regulation 2016/679, WP 259, p. 7.
[vii] Exemplul se regăsește în WP29, Guidelines on Consent under Regulation 2016/679, WP 259, p. 7.
[viii] WP29 Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, WP 217, p. 16-17.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

[ix] Ibid, p. 16.
[x] Voigt, P., von dem Bussche, A., The EU General Data Protection Regulation (GDPR) – A Practical Guide, Springer International Publishing (2017), p. 102.
[xi] European Data Protection. Law and Practice, Ed. Coord: Edurado Ustaran, CIPP/E, Partner, Hogan Lovells, IAPP (2018), p. 118
[xii] WP29 Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, WP 217, p. 16.
[xiii] Ibid, p. 20.
[xiv] Boardman, R., Mullock, J., Mole, A. Bird & Bird Guide to General Data Protection Regulation (2016), p. 10.
[xv] WP29 Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, WP 217, p. 19.
[xvi] Ibid, p. 19.
[xvii] Ibid, p. 20.
[xviii] Ibid, p. 19.
[xix] Ibid, p. 20.
[xx] European Data Protection. Law and Practice, Ed. Coord.: Edurado Ustaran, CIPP/E, Partner, Hogan Lovells, IAPP (2018), p. 119.
[xxi] WP29 Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, WP 217, p. 20-21.
[xxii] Ibid, p. 21.
[xxiii] Ibid, p. 21.
[xxiv] European Data Protection. Law and Practice, Ed. Coord.: Edurado Ustaran, CIPP/E, Partner, Hogan Lovells, IAPP (2018), p. 119.
[xxv] WP29 Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, WP 217, p. 23.
[xxvi] European Data Protection. Law and Practice, Ed. Coord.: Edurado Ustaran, CIPP/E, Partner, Hogan Lovells, IAPP (2018), p. 119.
[xxvii] WP29 Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, WP 217, p. 24.
[xxviii] Ibid, p. 33.
[xxix] European Data Protection. Law and Practice, Editor Coord.: Edurado Ustaran, CIPP/E, Partner, Hogan Lovells, IAPP (2018), p. 122.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

ProLegis

Prelucrarea Categoriilor Speciale de Date cu Caracter Personal

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

ProLegis

Cuprins

1. CADRU LEGAL 4

1.2. RGPD 4

2. CATEGORIILE SPECIALE DE DATE CU CARACTER PERSONAL ÎN CONFORMITATE CU RGPD 10

2.1. Logica din spatele definirii anumitor categorii de date cu caracter personal ca fiind speciale 10

2.2. Tipuri de categorii speciale de date cu caracter personal 11

2.3. Datele cu caracter personal referitoare la condamnări penale și infracțiuni 12

3. TEMEIURI LEGALE PENTRU PRELUCRAREA CATEGORIILOR SPECIALE DE DATE CU CARACTER PERSONAL 13

3.1. Consimțământul explicit 13

3.2. Obligațiile / drepturile specifice în domeniul ocupării forței de muncă și al securității sociale și protecției sociale 14

3.3. Interesele vitale ale persoanei vizate sau ale altei persoane fizice 15

3.4. Prelucrarea datelor de către un organism fără scop lucrativ și cu specific politic, filosofic, religios sau sindical 15

3.5. Datele făcute publice în mod manifest de către persoana vizată 15

3.6. Constatarea, exercitarea sau apărarea unui drept în instanță / instanțele care acționează în exercițiul funcției lor jurisdicționale 16

3.7. Interesul public major în baza dreptului Uniunii sau a dreptului intern 16

3.8. Medicina preventivă sau a muncii, evaluarea capacității de muncă a angajatului, stabilirea unui diagnostic medical, furnizarea de asistență medicală sau socială sau a unui tratament medical 16

3.9. Interesul public în domeniul sănătății publice 17

3.10. Prelucrarea în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice 17

3.11. Condițiile suplimentare din dreptul inern 17

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

4. CONCLUZIE ȘI RECOMANDĂRI 18
5. BIBLIOGRAFIE 18
Cărți 18
Documente referitoare la Grupul de lucru ”Articolul 29” 18
Link-uri web 18
6. NOTE 19

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

1. CADRU LEGAL

1.1. Carta drepturilor fundamentale a Uniunii Europene

Articolul 8

Protecția datelor cu caracter personal

1. Orice persoană are dreptul la protecția datelor cu caracter personal care o privesc.

2. Asemenea date trebuie tratate în mod corect, în scopurile precizate și ***pe baza consimțământului persoanei interesate sau în temeiul unui alt motiv legitim prevăzut de lege.*** *Orice persoană are dreptul de acces la datele colectate care o privesc, precum și dreptul de a obține rectificarea acestora.*

3. Respectarea acestor norme se supune controlului unei autorități independente.

1.2. RGPD

Considerentul (51)

Datele cu caracter personal care sunt, prin natura lor, deosebit de sensibile în ceea ce privește drepturile și libertățile fundamentale necesită o protecție specifică, deoarece contextul prelucrării acestora ar putea genera riscuri considerabile la adresa drepturilor și libertăților fundamentale. Aceste date cu caracter personal ar trebui să includă datele cu caracter personal care dezvăluie originea rasială sau etnică, utilizarea termenului „origine rasială" în prezentul regulament neimplicând o acceptare de către Uniune a teoriilor care urmăresc să stabilească existența unor rase umane separate. Prelucrarea fotografiilor nu ar trebui să fie considerată în mod sistematic ca fiind o prelucrare de categorii speciale de date cu caracter personal, întrucât fotografiile intră sub incidența definiției datelor biometrice doar în cazurile în care sunt prelucrate prin mijloace tehnice specifice care permit identificarea unică sau autentificarea unei persoane fizice. Asemenea date cu caracter personal nu ar trebui prelucrate, cu excepția cazului în care prelucrarea este permisă în cazuri specifice prevăzute de prezentul regulament, ținând seama de faptul că dreptul statelor membre poate prevedea dispoziții specifice cu privire la protecția datelor în scopul adaptării aplicării normelor din prezentul regulament în vederea respectării unei obligații legale sau a îndeplinirii unei sarcini care servește unui interes public sau care rezultă din exercitarea autorității publice cu care este învestit operatorul. Pe lângă cerințele specifice pentru o astfel de prelucrare, ar trebui să se aplice

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

principiile generale și alte norme prevăzute de prezentul regulament, în special în ceea ce privește condițiile pentru prelucrarea legală. Ar trebui prevăzute în mod explicit derogări de la interdicția generală de prelucrare a acestor categorii speciale de date cu caracter personal, printre altele atunci când persoana vizată își dă consimțământul explicit sau în ceea ce privește nevoile specifice în special atunci când prelucrarea este efectuată în cadrul unor activități legitime de către anumite asociații sau fundații al căror scop este de a permite exercitarea libertăților fundamentale.

Considerentul (52)

Derogarea de la interdicția privind prelucrarea categoriilor speciale de date cu caracter personal ar trebui să fie permisă, de asemenea, în cazul în care dreptul Uniunii sau dreptul intern prevede acest lucru și ar trebui să facă obiectul unor garanții adecvate, astfel încât să fie protejate datele cu caracter personal și alte drepturi fundamentale, atunci când acest lucru se justifică din motive de interes public, în special în cazul prelucrării datelor cu caracter personal în domeniul legislației privind ocuparea forței de muncă, protecția socială, inclusiv pensiile, precum și în scopuri de securitate, supraveghere și alertă în materie de sănătate, pentru prevenirea sau controlul bolilor transmisibile și a altor amenințări grave la adresa sănătății. Această derogare poate fi acordată în scopuri medicale, inclusiv sănătatea publică și gestionarea serviciilor de asistență medicală, în special în vederea asigurării calității și eficienței din punctul de vedere al costurilor ale procedurilor utilizate pentru soluționarea cererilor de prestații și servicii în cadrul sistemului de asigurări de sănătate, sau în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice. De asemenea, prelucrarea unor asemenea date cu caracter personal ar trebui permisă, printr-o derogare, atunci când este necesară pentru constatarea, exercitarea sau apărarea unui drept în justiție, indiferent dacă are loc în cadrul unei proceduri în fața unei instanțe sau în cadrul unei proceduri administrative sau a unei proceduri extrajudiciare.

Considerentul (53)

Categoriile speciale de date cu caracter personal care necesită un nivel mai ridicat de protecție ar trebui prelucrate doar în scopuri legate de sănătate atunci când este necesar pentru realizarea acestor scopuri în beneficiul persoanelor fizice și al societății în general, în special în contextul gestionării serviciilor și sistemelor de sănătate sau de asistență socială, inclusiv prelucrarea acestor date de către autoritățile de management și de către autoritățile centrale naționale din domeniul sănătății în scopul controlului calității, furnizării de informații de gestiune și al supravegherii generale a sistemului de sănătate sau de asistență socială la nivel național și local, precum și în contextul asigurării continuității

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

asistenței medicale sau sociale și a asistenței medicale transfrontaliere ori în scopuri de securitate, supraveghere și alertă în materie de sănătate ori în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice în temeiul dreptului Uniunii sau al dreptului intern, care trebuie să urmărească un obiectiv de interes public, precum și în cazul studiilor realizate în interes public în domeniul sănătății publice. Prin urmare, prezentul regulament ar trebui să prevadă condiții armonizate pentru prelucrarea categoriilor speciale de date cu caracter personal privind sănătatea, în ceea ce privește nevoile specifice, în special atunci când prelucrarea acestor date este efectuată în anumite scopuri legate de sănătate de către persoane care fac obiectul unei obligații legale de a păstra secretul profesional. Dreptul Uniunii sau dreptul intern ar trebui să prevadă măsuri specifice și adecvate pentru a proteja drepturile fundamentale și datele cu caracter personal ale persoanelor fizice. Statele membre ar trebui să aibă posibilitatea de a menține sau de a introduce condiții suplimentare, inclusiv restricții, în ceea ce privește prelucrarea datelor genetice, a datelor biometrice sau a datelor privind sănătatea. Totuși, acest lucru nu ar trebui să împiedice libera circulație a datelor cu caracter personal în cadrul Uniunii atunci când aceste condiții se aplică prelucrării transfrontaliere a unor astfel de date.

Considerentul (54)

Prelucrarea categoriilor speciale de date cu caracter personal poate fi necesară din motive de interes public în domeniile sănătății publice, fără consimțământul persoanei vizate. O astfel de prelucrare ar trebui condiționată de măsuri adecvate și specifice destinate să protejeze drepturile și libertățile persoanelor fizice. În acest context, conceptul de „sănătate publică" ar trebui interpretat astfel cum este definit în Regulamentul (CE) nr. 1338/2008 al Parlamentului European și al Consiliului (11), și anume toate elementele referitoare la sănătate și anume starea de sănătate, inclusiv morbiditatea sau handicapul, factorii determinanți care au efect asupra stării de sănătate, necesitățile în domeniul asistenței medicale, resursele alocate asistenței medicale, furnizarea asistenței medicale și asigurarea accesului universal la aceasta, precum și cheltuielile și sursele de finanțare în domeniul sănătății și cauzele mortalității. Această prelucrare a datelor privind sănătatea din motive de interes public nu ar trebui să ducă la prelucrarea acestor date în alte scopuri de către părți terțe, cum ar fi angajatorii sau societățile de asigurări și băncile.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

Considerentul (55)

În plus, prelucrarea datelor cu caracter personal de către autoritățile publice în vederea realizării obiectivelor prevăzute de dreptul constituțional sau de dreptul internațional public, ale asociațiilor religioase recunoscute oficial se efectuează din motive de interes public.

Considerentul (56)

În cazul în care, în cadrul activităților electorale, funcționarea sistemului democratic necesită, într-un stat membru, ca partidele politice să colecteze date cu caracter personal privind opiniile politice ale persoanelor, prelucrarea unor astfel de date poate fi permisă din motive de interes public, cu condiția să se prevadă garanțiile corespunzătoare.

Articolul 4

Definiții

În sensul prezentului regulament:

[…]

(13) ***„date genetice”*** *înseamnă datele cu caracter personal referitoare la caracteristicile genetice moștenite sau dobândite ale unei persoane fizice, care oferă informații unice privind fiziologia sau sănătatea persoanei respective și care rezultă în special în urma unei analize a unei mostre de material biologic recoltate de la persoana în cauză;*

(14) ***„date biometrice”*** *înseamnă o date cu caracter personal care rezultă în urma unor tehnici de prelucrare specifice referitoare la caracteristicile fizice, fiziologice sau comportamentale ale unei persoane fizice care permit sau confirmă identificarea unică a respectivei persoane, cum ar fi imaginile faciale sau datele dactiloscopice;*

(15) ***„date privind sănătatea”*** *înseamnă date cu caracter personal legate de sănătatea fizică sau mentală a unei persoane fizice, inclusiv prestarea de servicii de asistență medicală, care dezvăluie informații despre starea de sănătate a acesteia;*

Articolul 9

Prelucrarea de categorii speciale de date cu caracter personal

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

1. ***Se interzice prelucrarea de date cu caracter personal care dezvăluie originea rasială sau etnică, opiniile politice, confesiunea religioasă sau convingerile filozofice sau apartenența la sindicate și prelucrarea de date genetice, de date biometrice pentru identificarea unică a unei persoane fizice, de date privind sănătatea sau de date privind viața sexuală sau orientarea sexuală ale unei persoane fizice.***

2. ***Alineatul (1) nu se aplică*** *în următoarele situații:*

(a) persoana vizată și-a dat consimțământul explicit pentru prelucrarea acestor date cu caracter personal pentru unul sau mai multe scopuri specifice, cu excepția cazului în care dreptul Uniunii sau dreptul intern prevede ca interdicția prevăzută la alineatul (1) să nu poată fi ridicată prin consimțământul persoanei vizate;

(b) prelucrarea este necesară în scopul îndeplinirii obligațiilor și al exercitării unor drepturi specifice ale operatorului sau ale persoanei vizate în domeniul ocupării forței de muncă și al securității sociale și protecției sociale, în măsura în care acest lucru este autorizat de dreptul Uniunii sau de dreptul intern ori de un acord colectiv de muncă încheiat în temeiul dreptului intern care prevede garanții adecvate pentru drepturile fundamentale și interesele persoanei vizate;

(c) prelucrarea este necesară pentru protejarea intereselor vitale ale persoanei vizate sau ale unei alte persoane fizice, atunci când persoana vizată se află în incapacitate fizică sau juridică de a-și da consimțământul;

(d) prelucrarea este efectuată în cadrul activităților lor legitime și cu garanții adecvate de către o fundație, o asociație sau orice alt organism fără scop lucrativ și cu specific politic, filozofic, religios sau sindical, cu condiția ca prelucrarea să se refere numai la membrii sau la foștii membri ai organismului respectiv sau la persoane cu care acesta are contacte permanente în legătură cu scopurile sale și ca datele cu caracter personal să nu fie comunicate terților fără consimțământul persoanelor vizate;

(e) prelucrarea se referă la date cu caracter personal care sunt făcute publice în mod manifest de către persoana vizată;

(f) prelucrarea este necesară pentru constatarea, exercitarea sau apărarea unui drept în instanță sau ori de câte ori instanțele acționează în exercițiul funcției lor judiciare;

(g) prelucrarea este necesară din motive de interes public major, în baza dreptului Uniunii sau a dreptului intern, care este proporțional cu obiectivul urmărit, respectă esența

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

dreptului la protecția datelor și prevede măsuri corespunzătoare și specifice pentru protejarea drepturilor fundamentale și a intereselor persoanei vizate;

(h) prelucrarea este necesară în scopuri legate de medicina preventivă sau a muncii, de evaluarea capacității de muncă a angajatului, de stabilirea unui diagnostic medical, de furnizarea de asistență medicală sau socială sau a unui tratament medical sau de gestionarea sistemelor și serviciilor de sănătate sau de asistență socială, în temeiul dreptului Uniunii sau al dreptului intern sau în temeiul unui contract încheiat cu un cadru medical și sub rezerva respectării condițiilor și garanțiilor prevăzute la alineatul (3);

(i) prelucrarea este necesară din motive de interes public în domeniul sănătății publice, cum ar fi protecția împotriva amenințărilor transfrontaliere grave la adresa sănătății sau asigurarea de standarde ridicate de calitate și siguranță a asistenței medicale și a medicamentelor sau a dispozitivelor medicale, în temeiul dreptului Uniunii sau al dreptului intern, care prevede măsuri adecvate și specifice pentru protejarea drepturilor și libertăților persoanei vizate, în special a secretului profesional;

(j) prelucrarea este necesară în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice, în conformitate cu articolul 89 alineatul (1), în baza dreptului Uniunii sau a dreptului intern, care este proporțional cu obiectivul urmărit, respectă esența dreptului la protecția datelor și prevede măsuri corespunzătoare și specifice pentru protejarea drepturilor fundamentale și a intereselor persoanei vizate.

3. Datele cu caracter personal menționate la alineatul (1) pot fi prelucrate în scopurile menționate la alineatul (2) litera (h) în cazul în care datele respective sunt prelucrate de către un profesionist supus obligației de păstrare a secretului profesional sau sub responsabilitatea acestuia, în temeiul dreptului Uniunii sau al dreptului intern sau în temeiul normelor stabilite de organisme naționale competente sau de o altă persoană supusă, de asemenea, unei obligații de confidențialitate în temeiul dreptului Uniunii sau al dreptului intern ori al normelor stabilite de organisme naționale competente.

4. Statele membre pot menține sau introduce condiții suplimentare, inclusiv restricții, în ceea ce privește prelucrarea de date genetice, date biometrice sau date privind sănătatea.

Articolul 10

Prelucrarea de date cu caracter personal referitoare la condamnări penale și infracțiuni

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

Prelucrarea de date cu caracter personal referitoare la condamnări penale și infracțiuni sau la măsuri de securitate conexe *în temeiul articolului 6 alineatul (1) se efectuează* ***numai sub controlul unei autorități de stat sau atunci când prelucrarea este autorizată de dreptul Uniunii sau de dreptul intern*** *care prevede garanții adecvate pentru drepturile și libertățile persoanelor vizate. Orice registru cuprinzător al condamnărilor penale se ține numai sub controlul unei autorități de stat.*

2. CATEGORIILE SPECIALE DE DATE CU CARACTER PERSONAL ÎN CONFORMITATE CU RGPD

2.1. Logica din spatele definirii anumitor categorii de date cu caracter personal ca fiind speciale

Încă din perioada redactării primului act juridic al UE privind protecția datelor cu caracter personal – Directiva 95/46 – Comisia Europeană a subliniat că prelucrarea anumitor categorii de date cu caracter personal ar putea pune în pericol drepturile și libertățile fundamentale ale cetățenilor europeni[i]. Astfel, a fost stabilită o interdicție generală pentru prelucrarea categoriilor „riscante” de date cu caracter personal. Acestea au fost numite „categorii speciale de date cu caracter personal”, însă în practică au fost denumite „date sensibile” având în vedere natura lor sensibilă pentru sfera privată a individului[ii]. Asemenea date pot fi prelucrate numai în circumstanțe excepționale, enumerate în mod exhaustiv în legislația privind protecția datelor din statele membre.

RGPD continuă această abordare, însă lărgește sfera de aplicabilitate a categoriilor speciale de date cu caracter personal și prevede noi excepții (temeiuri juridice) care le conferă operatorilor dreptul la prelucrare.

Trebuie menționat faptul că tipuri diferite de date au un impact diferit asupra indivizilor. Ce date sunt definite drept sensibile se bazează pe un principiu obiectiv și nu pe unul subiectiv. Altfel spus, cuiva i s-ar putea părea sensibile datele privind situația financiară, istoricul sancțiunilor disciplinare sau codul numeric personal. Cu toate acestea, dacă astfel de date nu sunt recunoscute de către legiuitorul european ca fiind sensibile, atunci ele nu intră sub incidența regimului special de prelucrare, indiferent dacă din punct de vedere subiectiv sunt considerate sensibile.

La nivel teoretic se arată că alegerea cu privire la ce categorii de date cu caracter personal ar trebui definite ca fiind speciale a fost semnificativ influențată de legile anti-discriminare, ceea ce explică de ce date precum codul numeric personal sau detaliile cardurilor de credit nu sunt catalogate drept sensibile[iii].

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

2.2. Tipuri de categorii speciale de date cu caracter personal

Potrivit articolului 9, alineatul (1) al RGPD, următoarele tipuri de date cu caracter personal sunt considerate categorii speciale (date sensibile):

- **Datele cu caracter personal care dezvăluie originea rasială sau etnică** = această categorie de date este considerată sensibilă, deoarece implică un grad ridicat de discriminare. În teoria dreptului sunt oferite următoarele exemple de date care ar putea intra în această categorie: numele și prenumele persoanei, locul nașterii, limba maternă sau numele părinților, care, dacă sunt combinate, permit formularea de concluzii cu privire la originea sa[iv];
- **Opiniile politice** = aceste date merită o protecție specială, deoarece le garantează cetățenilor dreptul de a-și forma opinii cu privire la politică și, totodată, de a participa la viața politică a țării (în mod activ, ca politicieni și / sau pasiv, ca alegători sau membri ai societății civile). Astfel de date cuprind informații despre apartenența la partidele politice, aderarea la petiții, participarea la demonstrații, reuniuni politice sau alte evenimente similare, informații privind susținerea sau respingerea unei anumite idei politice[v];
- **Confesiunea religioasă sau convingerile filosofice** = aceste categorii de date se află în strânsă legătură cu libertatea conștiinței, adică libertatea de a decide dacă să credem în forțe transcendentale care ne determină viața de zi cu zi și dacă să o manifestăm sau nu. Istoria omenirii este plină de exemple în care violența a luat naștere din cauza diferențelor religioase, astfel încât aceste date ar trebui protejate în mod special;
- **Apartenența la sindicate** = informațiile referitoare la membrii de sindicat sunt sensibile, deoarece pot da naștere unor tratamente discriminatorii în domeniul legislației muncii. Cetățenii europeni sunt liberi să negocieze și să acționeze în mod colectiv și, în consecință, nu ar trebui să fie tratați inegal în baza afilierii lor sindicale[vi];
- **Datele genetice** = reprezintă o nouă categorie de date sensibile introduse de RGPD și care sunt definite drept „date cu caracter personal referitoare la caracteristicile genetice moștenite sau dobândite ale unei persoane fizice, care oferă informații unice privind fiziologia sau sănătatea persoanei respective și care rezultă în special în urma unei analize a unei mostre de material biologic recoltate de la persoana în cauză”. Unele state membre au catalogat deja drept sensibil acest tip de date[vii], însă RGPD îl introduce pentru prima dată la nivelul UE. Datele genetice ar trebui protejate, deoarece se referă nu numai la persoana vizată, ci și la rudele acesteia (de pildă, datele persoanelor decedate, datele copiilor etc.). Mai mult decât atât, analiza detaliată a unor asemenea date poate dezvălui alte tipuri

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

de informații sensibile, cum ar fi datele psihologice sau de sănătate (de exemplu, predispoziția la boli, vulnerabilitatea etc.);

- **Datele biometrice pentru identificarea unică a unei persoane fizice** = astfel de tipuri de date necesită protecție, întrucât le permit operatorilor să identifice fără echivoc o persoană pe baza caracteristicilor fizice sau comportamentale: amprente, recunoaștere facială, iris, retină, modele vasculare, ADN, vorbire, semnătură etc. Având în vedere că prelucrarea acestor tipuri de date a ajuns să fie din ce în ce mai frecvent utilizată odată cu dezvoltările tehnologice (de exemplu, sisteme pentru controlarea accesului în clădiri, sisteme de identificare pe dispozitive la distanță , precum telefoane mobile, tablete etc.), a trebuit să devină mai restrictivă și supusă controlului, motiv pentru care a și fost inclusă în lista datelor „sensibile" din RGPD. Contrar practicilor stabilite în unele state membre, prelucrarea fotografiilor nu este automat considerată sensibilă. Fotografiile sunt considerate date sensibile numai dacă permit identificarea sau autentificarea biometrică a unei persoane (de exemplu, într-un pașaport sau alt tip de document de identitate)[viii];
- **Datele privind sănătatea sau datele privind viața sexuală sau orientarea sexuală** = aceste date sunt foarte sensibile, deoarece au legătură cu cele mai intime aspecte ale vieții individului. În plus, informațiile privind viața sexuală și orientarea sexuală pot conduce la discriminări, manipulări etc. La nivel teoretic se recomandă ca aceste date să includă și identitatea exactă a partenerului / partenerilor individului[ix].

2.3. Datele cu caracter personal referitoare la condamnări penale și infracțiuni

Datele referitoare la condamnări penale și infracțiuni sau măsurile de securitate conexe **nu sunt** declarate o categorie specială de date cu caracter personal. Totuși, legislația anumitor state membre le consideră sensibile[x]. Cu toate acestea, astfel de informații pot conduce la tratament inegal (bunăoară, în domeniul ocupării forței de muncă), astfel încât fac și ele obiectul unor norme speciale de prelucrare. RGPD nu introduce modificări semnificative cu privire la vechea directivă 95/46 în ceea ce privește datele referitoare la condamnări penale și infracțiuni. În același timp, având în vedere că normele directivei au fost transpuse în moduri diferite de către statele membre, RGPD introduce o abordare mai generală, la nivelul UE. Conform articolului 10 din RGPD, aceste date pot fi prelucrate în baza unuia dintre temeiurile expuse în articolul 6, cu condiția să fie îndeplinită una dintre următoarele cerințe suplimentare **alternative**:

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

(i) Prelucrarea trebuie să fie efectuată numai sub controlul unei autorități de stat, sau

(ii) Prelucrarea trebuie să fie autorizată de dreptul Uniunii sau de dreptul intern care prevede garanții adecvate pentru drepturile și libertățile persoanelor vizate.

Există o incertitudine în legătură cu această dispoziție, deoarece nu este clar cum se aplică aceste două cerințe suplimentare împreună cu articolul 6. Potrivit interpretării conservatoare, entitățile private sau comerciale nu pot prelucra astfel de date, altfel spus, „nu este loc în regulament pentru prelucrarea privată sau comericală a acestor date”[xi]. Cealaltă interpretare afirmă că acest tip de date poate fi prelucrat în baza tuturor temeiurilor legale posibile, numai dacă sunt îndeplinite cerințele suplimentare. Din punct de vedere teoretic, această prevedere ar conduce probabil la o divergență națională continuă[xii]. Deși autoritățile locale (AL) vor acționa în calitate de autorități publice și ar putea justifica teoretic prima cerință suplimentară, este recomandabil să fie examinate reglementările locale atunci când astfel de tipuri de date urmează să fie prelucrate (în special în ceea ce privește activitățile de resurse umane și colectarea cazierelor judiciare, deoarece AL acționează în acest context ca angajator, nu ca titular al puterii publice, iar aplicabilitatea primei condiții este discutabilă).

3. TEMEIURI LEGALE PENTRU PRELUCRAREA CATEGORIILOR SPECIALE DE DATE CU CARACTER PERSONAL

Interdicția generală de prelucrare a categoriilor speciale de date cu caracter personal nu se aplică, cu condiția să fie îndeplinită una dintre cerințele **alternative** de mai jos:

3.1. Consimțământul explicit

Cerințele care trebuie îndeplinite în conformitate cu RGPD pentru a avea un consimțământ valabil (acordat în mod liber, specific, în cunoștință de cauză, lipsit de ambiguitate) se aplică în oricare dintre cazurile de prelucrare a categoriilor speciale de date. Termenul „explicit” nu este definit în RGPD. WP29 afirmă că este necesar un consimțământ explicit în situațiile în care protecția datelor devine riscantă, impunându-se astfel un nivel sporit de control asupra datelor cu caracter personal[xiii].

Termenul „explicit” se referă la modul în care consimțământul este exprimat de persoana vizată – aceasta trebuie să își declare în mod expres consimțământul[xiv]. Una dintre modalitățile de acordare a consimțământului este confirmarea prin intermediul unei

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

declarații scrise. În mediul online pot fi folosite diverse soluții, cum ar fi: completarea unui formular electronic, trimiterea unui e-mail, încărcarea unui document scanat cu semnătura persoanei vizate sau utilizarea semnăturii electronice. Orice mijloace care i-ar da posibilitatea operatorului să demonstreze obținerea corespunzătoare a consimțământului sunt adecvate.

Din cauza dezechilibrului de putere dintre autoritățile publice și persoanele vizate, nu este recomandabil ca AL să se bazeze în principal pe consimțământul explicit în scopul prelucrării categoriilor speciale de date cu caracter personal (inclusiv în relațiile cu cetățenii și angajații).

3.2. Obligațiile / drepturile specifice în domeniul ocupării forței de muncă și al securității sociale și protecției sociale

Această condiție are o relevanță deosebită pentru AL atunci când gestionează procesul intern de resurse umane. Prelucrarea categoriilor speciale de date cu caracter personal poate fi necesară în fiecare etapă a raporturilor de muncă – de la momentul instituirii (procesul de angajare a noului personal), la realizarea și modificările survenite pe durata perioadei contractuale, și până la încetarea raporturilor respective.

Printre situațiile în care prelucrarea poate fi necesară se numără: acordarea de concedii medicale / de materniate, transferarea angajatului pe o poziție mai adecvată din considerente de sănătate la cererea autorităților din domeniul sănătății, respectarea normelor care prevăd protecția specială a anumitor categorii de salariați în cazul încetării raporturilor de muncă etc.

Cerințele generale introduse în RGPD pentru aplicarea acestui temei sunt:

(i) Prelucrarea să fie necesară pentru îndeplinirea unei obligații a operatorului de date sau respectarea unui drept al persoanei vizate;
(ii) Obligația / dreptul să fie stabilite în dreptul UE / intern sau printr-un acord colectiv de muncă;
(iii) Să fie garantată respectarea drepturilor fundamentale și intereselor persoanei vizate.

Pentru a aplica acest temei juridic, este necesar să fie respectată legislația specifică a statutului membru în care AL funcționează ca angajator. Dat fiind că în ceea ce privește legislația muncii RGPD autorizează statele membre să adopte norme mai detaliate cu privire la protecția datelor cu caracter personal (conform articolului 88), se recomandă o abordare punctuală din partea autorității atunci când pune în aplicare acest temei.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

3.3. Interesele vitale ale persoanei vizate sau ale altei persoane fizice

Similar cu temeiul juridic prevăzut în articolul 6, alineatul (1), punctul (d) din RGPD, astfel de situații se referă la circumstanțe de viață sau moarte[xv]. Interesul vital poate aparține fie persoanei vizate, fie unei alte persoane. Deosebirea față de articolul 6 constă în faptul că operatorul are sarcina de a demonstra existența unei condiții suplimentare, și anume că „persoana vizată se află în incapacitate fizică sau juridică de a-și da consimțământul". Această formulare presupune că operatorul ar trebui să încerce mai întâi să obțină consimțământul persoanei vizate[xvi].

3.4. Prelucrarea datelor de către un organism fără scop lucrativ și cu specific politic, filosofic, religios sau sindical

În baza acestui temei pot prelucra date sensibile anumite organizații non-profit, cum ar fi: partidele politice, fundațiile, bisericile, alte forme de organizații filosofice, religioase sau sindicale. Astfel de organizații pot prelucra date sensibile dacă:

(i) datele se referă strict la membrii / foștii membri sau la persoanele care mențin un contact periodic;
(ii) prelucrarea face parte din activitățile lor legitime;
(iii) prelucrarea se desfășoară în corelație cu scopurile lor specifice;
(iv) există garanții adecvate pentru respectarea drepturilor persoanelor vizate;
(v) datele cu caracter personal nu sunt dezvăluite altor organizații fără consimțământul persoanelor vizate.

În dreptul intern se pot regăsi alte cerințe specifice[xvii].

Acest temei juridic nu are aproape nicio aplicație pentru activitățile din cadrul AL.

3.5. Datele făcute publice în mod manifest de către persoana vizată

În cazul în care datele cu caracter personal sunt dezvăluite în mod vădit publicului larg de către persoana vizată, se presupune că aceasta a renunțat la protecția specială asigurată acestor informații. În orice caz, decizia de a dezvălui astfel de informații trebuie să fie rezultatul alegerii libere a persoanei[xviii]. Dezvăluirile pot viza diverse lucruri – date din registre publice, site-uri web, liste, forumuri sau chiar profiluri ale unor rețele sociale accesibile fără cont de utilizator etc.[xix]. Faptul că astfel de date sunt făcute publice în mod manifest nu îl scutesc pe operator de obligația respectării celorlalte cerințe din RGPD – de exemplu, respectarea principiilor privind protecția datelor, respectarea confidențialității, luarea măsurilor adecvate pentru garantarea securității datelor etc.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

3.6. Constatarea, exercitarea sau apărarea unui drept în instanță / instanțele care acționează în exercițiul funcției lor jurisdicționale

În anumite cazuri, prelucrarea datelor sensibile poate fi necesară pentru constatarea, execritarea sau apărarea unui drept în justiție. Operatorului îi revine sarcina de a dovedi că o astfel de prelucrare trebuie efectuată, că există o legătură strânsă și substanțială între prelucrare și scopuri[xx]. Astfel de situații pot include, de exemplu: recursul în fața instanțelor administrative pentru actele emise de AL în cazul în care au fost prelucrate date sensibile în cadrul procedurii administrative anterioare; conflictele de muncă în care datele privind sănătatea angajaților ar fi trebuit luate în considerare de către AL ca angajator etc.

În plus, prelucrarea din cadrul activităților judiciare ale instanțelor poate să justifice prelucrarea unor asemenea categorii de date cu caracter personal.

3.7. Interesul public major în baza dreptului Uniunii sau a dreptului intern

RGPD autorizează statele membre să introducă în legislația națională ipoteze specifice pentru prelucrări de date sensibile justificate în baza temeiului interesului public major.

În orice caz, pentru a îndeplini cerințele RGPD, statele membre trebuie să se asigure că:

(i) prelucrarea este proporțională cu obiectivul urmărit;
(ii) este respectată esența dreptului la protecția datelor;
(iii) legislația adoptată prevede măsuri corespunzătoare și specifice pentru protejarea drepturilor fundamentale și a intereselor persoanei vizate.

Rămâne de văzut cum va fi folosită această oportunitate pe viitor. Se recomandă ca AL să analizeze de la caz la caz dacă se poate baza pe acest temei.

3.8. Medicina preventivă sau a muncii, evaluarea capacității de muncă a angajatului, stabilirea unui diagnostic medical, furnizarea de asistență medicală sau socială sau a unui tratament medical

Interdicția de a prelucra categorii speciale de date cu caracter personal nu se aplică prelucrării în scopuri medicale / sociale[xxi]. O astfel de prelucrare poate avea loc în diferite domenii, cum ar fi: medicina muncii, diagnosticările medicale, serviciile de asistență socială sau medicală. Prelucrările de acest gen pot fi efectuate fie în temeiul dreptului Uniunii / dreptului intern, fie în baza unui contract cu un profesionist în domeniul sănătății (medic)[xxii]. În plus, articolul 9, alineatul (3) din RGPD permite prelucrarea datelor sensibile de către un profesionist supus obligației de păstrare a secretului profesional.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

Acest temei juridic se aplică medicilor, asistentelor medicale și altor persoane implicate în furnizarea de servicii de asistență medicală sau socială[xxiii].

Din punct de vedere practic, această dispoziție permite AL, în calitatea lor de angajatori, să asigure servicii de medicina muncii ca parte a obligației mai cuprinzătoare de a asigura condiții de muncă sigure și care să nu pericliteze sănătatea.

3.9. Interesul public în domeniul sănătății publice

Conform considerentului 54 din RGPD „sănătatea publică" ar trebui interpretată în conformitate cu definiția Regulamentului (CE) nr. 1338/2008, mai precis tot ceea ce ține de sănătate: starea de sănătate, inclusiv morbididatea și dizabilitatea, factorii determinanți care au un efect asupra stării de sănătate, nevoile de menținere a sănătății, resursele alocate pentru asistența medicală, furnizarea de asistență medicală și accesul universal la aceasta, finanțarea domeniului asistenței medicale, precum și cauzele mortalității.

Motivele care pot justifica aplicarea acestui temei juridic includ protecția împotriva amenințărilor transfrontaliere grave la adresa sănătății sau asigurarea de standarde ridicate de calitate și siguranță a asistenței medicale și a medicamentelor sau a dispozitivelor medicale[xxiv].

Prelucrarea datelor de sănătate din motive de interes public nu ar trebui să ducă la prelucrarea datelor cu caracter personal în alte scopuri de către terți, cum ar fi angajatorii sau companiile de asigurări și bancare.

3.10. Prelucrarea în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice

Prelucrarea în astfel de scopuri ar trebui să fie făcută în în temeiul dreptului Uniunii / dreptului intern. RGPD prevede că dispozițiile legislative care permit o astfel de prelucrare trebuie să fie proporționale cu obiectivul urmărit, să respecte esența dreptului la protecție a datelor și să prevadă măsuri adecvate și specifice pentru protejarea drepturilor fundamentale și intereselor persoanei vizate. Garanțiile introduse trebuie să corespundă naturii sensibile a datelor în cauză[xxv].

3.11. Condițiile suplimentare din dreptul inern

Articolul 9, alineatul (4) al RGPD autorizează statele membre să introducă și alte condiționări sau limitări pentru prelucrarea anumitor categorii speciale de date cu caracter personal, mai exact pentru: datele genetice, datele biometrice sau datele privind sănătatea. În acest sens, legislația care se aplică AL ar trebui monitorizată pe viitor.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

4. CONCLUZIE ȘI RECOMANDĂRI

AL ar trebui să fie conștiente de faptul că anumite categorii de date cu caracter personal merită o protecție specială, deoarece vizează direct sferele private cele mai intime și / sau implică riscul de discriminare. Ca regulă generală, prelucrarea acestor date este interzisă, cu excepția cazului în care există condiții suplimentare (care fac excepția de la această regulă).

Cele mai practice aspecte care ar putea să afecteze activitățile AL vizează prelucrarea datelor de sănătate ale angajaților. RGPD permite o astfel de prelucrare, însă numai dacă este necesară în temeiul legislației muncii în scopul exercitării obligațiilor operatorului sau al respectării drepturilor persoanei vizate.

Datele privind condamnările penale și infracțiunile nu fac parte propriu-zis din categoriile speciale, însă sunt tratate în regim special în cadrul RGPD. Practicile din domeniul resurselor umane pentru colectarea cazierului judiciar sau efectuarea unor controale extinse asupra viitorilor angajați ar trebui revizuite în lumina prevederilor RGPD.

5. BIBLIOGRAFIE

Cărți

- **Boardman, R., Mullock, J., Mole, A.** Bird & Bird Guide to General Data Protection Regulation (2016);
- **Ehmann, E., Helfrich, M.** EG Datenschutzrichtlinie: Kurzkommentar, Verlag Dr. Otto Schmidt, Koln, (1999)
- **Voigt, P., von dem Bussche, A.**, The EU General Data Protection Regulation (GDPR) – A Practical Guide, Springer International Publishing (2017);
- **EU** General Data Protection Regulation (GDPR). An Implementation and Compliance Guide, IT Governance Publishing, Cambridgeshire (2016);
- **European** Data Protection. Law and Practice, Ed.coord.: Edurado Ustaran, CIPP/E, Partner, Hogan Lovells, IAPP (2018);

Documente referitoare la Grupul de lucru ”Articolul 29”

- WP29, Guidelines on Consent under Regulation 2016/679, WP 259;
- WP29, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, WP 217;

Link-uri web

- http://europa.eu/rapid/press-release_IP-18-386_en.htm

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

- https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en
- https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/sensitive-data/what-personal-data-considered-sensitive_en
- https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/sensitive-data/under-what-conditions-can-my-company-organisation-process-sensitive-data_en

6. NOTE

[i] Ehmann, E., Helfrich, M. EG Datenschutzrichtlinie: Kurzkommentar, Verlag Dr. Otto Schmidt, Koln, (1999), p. 130-131.
[ii] RGPD recunoște în mod explicit termenul „date sensibile" – a se vedea Considerentul 10.
[iii] European Data Protection. Law and Practice, Ed.coord.: Edurado Ustaran, CIPP/E, Partner, Hogan Lovells, IAPP (2018), p. 123.
[iv] Voigt, P., von dem Bussche, A., The EU General Data Protection Regulation (GDPR) – A Practical Guide, Springer International Publishing (2017), p. 111.
[v] Ibid, p. 111.
[vi] Ibid, p. 111.
[vii] În Bulgaria astfel de date sunt considerate sensibile încă din anul 2005.
[viii] Boardman, R., Mullock, J., Mole, A. Bird & Bird Guide to General Data Protection Regulation (2016), p. 18.
[ix] Voigt, P., von dem Bussche, A., The EU General Data Protection Regulation (GDPR) – A Practical Guide, Springer International Publishing (2017), p. 111.
[x] Boardman, R., Mullock, J., Mole, A. Bird & Bird Guide to General Data Protection Regulation (2016), p. 19.
[xi] EU General Data Protection Regulation (GDPR). An Implementation and Compliance Guide, IT Governance Publishing, Cambridgeshire (2016), p. 196.
[xii] Boardman, R., Mullock, J., Mole, A. Bird & Bird Guide to General Data Protection Regulation (2016), p. 19.
[xiii] WP29, Guidelines on Consent under Regulation 2016/679, WP 259, p. 18.
[xiv] Ibid, p. 18.
[xv] European Data Protection. Law and Practice, Ed.coord: Edurado Ustaran, CIPP/E, Partner, Hogan Lovells, IAPP (2018), p. 126.
[xvi] Ibid, p. 126.
[xvii] Ibid, p. 126-127.
[xviii] Voigt, P., von dem Bussche, A., The EU General Data Protection Regulation (GDPR) – A Practical Guide, Springer International Publishing (2017), p. 113.
[xix] Ibid, p. 113.
[xx] European Data Protection. Law and Practice, Executive Editor: Edurado Ustaran, CIPP/E, Partner, Hogan Lovells, IAPP (2018), p. 127.
[xxi] Ibid, p. 128.
[xxii] Ibid, p. 129.
[xxiii] Ibid, p. 129.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

[xxiv] Voigt, P., von dem Bussche, A., The EU General Data Protection Regulation (GDPR) – A Practical Guide, Springer International Publishing (2017), p. 114.
[xxv] Ibid, p. 115.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

ProLegis

Desemnarea, Funcția și Sarcinile Responsabililor cu Protecția Datelor (RPD)

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

ProLegis

Cuprins

1. CADRU LEGAL 4

RGPD 4

2. DESEMNAREA RPD 7

2.1. Numirea obligatorie în conformitate cu RGPD 7

2.1.1. Autoritatea publică sau organismul public 7

2.1.2. Activitățile principale ale operatorului sau ale persoanei împuternicite de operator […] necesită o monitorizare periodică și sistematică a persoanelor vizate pe scară largă 8

2.1.3. Activitățile principale ale operatorului sau ale persoanei împuternicite de operator constau în prelucrarea pe scară largă a unor categorii speciale de date […] sau a unor date cu caracter personal privind condamnări penale și infracțiuni 9

2.2. Alte situații de numire a RPD 10

2.2.1. Numirea obligatorie în conformitate cu dreptul Uniunii sau cu dreptul intern 10

2.2.2. Numirea voluntară 10

2.3. Relațiile contractuale cu RPD 10

2.3.1. Contractul de muncă 10

2.3.2. Contractul de servicii 11

3. FUNCȚIA RPD 11

3.1. Implicarea în toate chestiunile legate de protecția datelor cu caracter personal 11

3.2. Asigurarea resurselor necesare și a independenței 12

3.3. Conflictul de interese 13

4. SARCINILE RPD 13

4.1. Monitorizarea 13

4.2. EIPD 14

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

4.3. Punctul de contact 14
4.4. Păstrarea evidenței 15
5. CONCLUZIE ȘI RECOMANDĂRI 15
6. BIBLIOGRAFIE 16
Cărți 16
Documente referitoare la Grupul de lucru ”Articolul 29” 16
Link-uri web 16
7. NOTE 16

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

1. CADRU LEGAL

RGPD

Considerentul (97)

În cazul în care prelucrarea este efectuată de o autoritate publică, cu excepția instanțelor sau a autorităților judiciare independente atunci când acționează în calitatea lor judiciară, în cazul în care, în sectorul privat, prelucrarea este efectuată de un operator a cărui activitate principală constă în operațiuni de prelucrare care necesită o monitorizare regulată și sistematică a persoanelor vizate pe scară largă, sau în cazul în care activitatea principală a operatorului sau a persoanei împuternicite de operator constă în prelucrarea pe scară largă de categorii speciale de date cu caracter personal și de date privind condamnările penale și infracțiunile, o persoană care deține cunoștințe de specialitate în materie de legislație și practici privind protecția datelor ar trebui să acorde asistență operatorului sau persoanei împuternicite de operator pentru monitorizarea conformității, la nivel intern, cu prezentul regulament. În sectorul privat, activitățile principale ale unui operator se referă la activitățile sale de bază, și nu la prelucrarea datelor cu caracter personal drept activități auxiliare. Nivelul necesar al cunoștințelor de specialitate ar trebui să fie stabilit în special în funcție de operațiunile de prelucrare a datelor efectuate și de nivelul de protecție impus pentru datele cu caracter personal prelucrate de operator sau de persoana împuternicită de operator. Acești responsabili cu protecția datelor, indiferent dacă sunt sau nu angajați ai operatorului, ar trebui să fie în măsură să își îndeplinească atribuțiile și sarcinile în mod independent.

Articolul 37

Desemnarea responsabilului cu protecția datelor

1. Operatorul și persoana împuternicită de operator desemnează un responsabil cu protecția datelor ori de câte ori:

(a) prelucrarea este efectuată de o autoritate sau un organism public, cu excepția instanțelor care acționează în exercițiul funcției lor jurisdicționale;

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

(b) activitățile principale ale operatorului sau ale persoanei împuternicite de operator constau în operațiuni de prelucrare care, prin natura, domeniul de aplicare și/sau scopurile lor, necesită o monitorizare periodică și sistematică a persoanelor vizate pe scară largă; sau

(c) activitățile principale ale operatorului sau ale persoanei împuternicite de operator constau în prelucrarea pe scară largă a unor categorii speciale de date, menționată la articolul 9, sau a unor date cu caracter personal privind condamnări penale și infracțiuni, menționată la articolul 10.

2. Un grup de întreprinderi poate numi un responsabil cu protecția datelor unic, cu condiția ca responsabilul cu protecția datelor să fie ușor accesibil din fiecare întreprindere.

3. În cazul în care operatorul sau persoana împuternicită de operator este o autoritate publică sau un organism public, poate fi desemnat un responsabil cu protecția datelor unic pentru mai multe dintre aceste autorități sau organisme, luând în considerare structura organizatorică și dimensiunea acestora.

4. În alte cazuri decât cele menționate la alineatul (1), operatorul sau persoana împuternicită de operator ori asociațiile și alte organisme care reprezintă categorii de operatori sau de persoane împuternicite de operatori pot desemna sau, acolo unde dreptul Uniunii sau dreptul intern solicită acest lucru, desemnează un responsabil cu protecția datelor. Responsabilul cu protecția datelor poate să acționeze în favoarea unor astfel de asociații și alte organisme care reprezintă operatori sau persoane împuternicite de operatori.

5. Responsabilul cu protecția datelor este desemnat pe baza calităților profesionale și, în special, a cunoștințelor de specialitate în dreptul și practicile din domeniul protecției datelor, precum și pe baza capacității de a îndeplini sarcinile prevăzute la articolul 39.

6. Responsabilul cu protecția datelor poate fi un membru al personalului operatorului sau persoanei împuternicite de operator sau poate să își îndeplinească sarcinile în baza unui contract de servicii.

7. Operatorul sau persoana împuternicită de operator publică datele de contact ale responsabilului cu protecția datelor și le comunică autorității de supraveghere.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

Articolul 38

Funcția responsabilului cu protecția datelor

1. Operatorul și persoana împuternicită de operator se asigură că responsabilul cu protecția datelor este implicat în mod corespunzător și în timp util în toate aspectele legate de protecția datelor cu caracter personal.

2. Operatorul și persoana împuternicită de operator sprijină responsabilul cu protecția datelor în îndeplinirea sarcinilor menționate la articolul 39, asigurându-i resursele necesare pentru executarea acestor sarcini, precum și accesarea datelor cu caracter personal și a operațiunilor de prelucrare, și pentru menținerea cunoștințelor sale de specialitate.

3. Operatorul și persoana împuternicită de operator se asigură că responsabilul cu protecția datelor nu primește niciun fel de instrucțiuni în ceea ce privește îndeplinirea acestor sarcini. Acesta nu este demis sau sancționat de către operator sau de persoana împuternicită de operator pentru îndeplinirea sarcinilor sale. Responsabilul cu protecția datelor răspunde direct în fața celui mai înalt nivel al conducerii operatorului sau persoanei împuternicite de operator.

4. Persoanele vizate pot contacta responsabilul cu protecția datelor cu privire la toate chestiunile legate de prelucrarea datelor lor și la exercitarea drepturilor lor în temeiul prezentului regulament.

5. Responsabilul cu protecția datelor are obligația de a respecta secretul sau confidențialitatea în ceea ce privește îndeplinirea sarcinilor sale, în conformitate cu dreptul Uniunii sau cu dreptul intern.

6. Responsabilul cu protecția datelor poate îndeplini și alte sarcini și atribuții. Operatorul sau persoana împuternicită de operator se asigură că niciuna dintre aceste sarcini și atribuții nu generează un conflict de interese.

Articolul 39

Sarcinile responsabilului cu protecția datelor

1. Responsabilul cu protecția datelor are cel puțin următoarele sarcini:

(a) informarea și consilierea operatorului, sau a persoanei împuternicite de operator, precum și a angajaților care se ocupă de prelucrare cu privire la obligațiile care le revin

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

în temeiul prezentului regulament și al altor dispoziții de drept al Uniunii sau drept intern referitoare la protecția datelor;

(b) monitorizarea respectării prezentului regulament, a altor dispoziții de drept al Uniunii sau de drept intern referitoare la protecția datelor și a politicilor operatorului sau ale persoanei împuternicite de operator în ceea ce privește protecția datelor cu caracter personal, inclusiv alocarea responsabilităților și acțiunile de sensibilizare și de formare a personalului implicat în operațiunile de prelucrare, precum și auditurile aferente;

(c) furnizarea de consiliere la cerere în ceea ce privește evaluarea impactului asupra protecției datelor și monitorizarea funcționării acesteia, în conformitate cu articolul 35;

(d) cooperarea cu autoritatea de supraveghere;

(e) asumarea rolului de punct de contact pentru autoritatea de supraveghere privind aspectele legate de prelucrare, inclusiv consultarea prealabilă menționată la articolul 36, precum și, dacă este cazul, consultarea cu privire la orice altă chestiune.

2. În îndeplinirea sarcinilor sale, responsabilul cu protecția datelor ține seama în mod corespunzător de riscul asociat operațiunilor de prelucrare, luând în considerare natura, domeniul de aplicare, contextul și scopurile prelucrării.

2. DESEMNAREA RPD

2.1. Numirea obligatorie în conformitate cu RGPD

2.1.1. Autoritatea publică sau organismul public

RGPD nu definește ce se înțelege prin „autoritatea publică sau organismul public”. Definirea unei persoană fizice / juridice ca autoritate / organism public ar trebui făcută în conformitate cu legislația națională a fiecărui stat membru. Acest concept ar trebui interpretat **în sens larg**, incluzând autoritățile naționale, regionale și **locale**. Potrivit WP29, conceptul vizează și anumite persoane fizice / juridice ale căror activități sunt reglementate de dreptul public / privat (de exemplu, serviciile de transport public, aprovizionarea cu apă și energie, infrastructura rutieră, radiodifuziunea publică, locuințele publice sau organismele disciplinare pentru profesiile reglementate)[i]. Logica unei astfel de interpretări este că persoanele vizate (cetățenii) au o posibilitate limitată de a alege dacă și cum vor fi prelucrate datele lor personale de asemenea entități. Deși o astfel de interpretare nu este impusă și nu creează obligații, se recomandă să se analizeze cu atenție în cadrul acestor organizații dacă este cazul să fie numiți RPD.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

Trebuie menționat că WP29 propune ca bună practică desemnarea RPD ale cărui funcții să acopere toate operațiunile de prelucrare efectuate, inclusiv cele care nu au legătură cu îndeplinirea unei sarcini publice sau cu exercitarea atribuțiilor oficiale (de exemplu, relațiile cu angajații)[ii]. Cu toate acestea, niciuna dintre prevederile RGPD nu impune numirea RPD numai pentru activitățile de prelucrare legate de funcțiile publice. În acest sens, o interpretare mai rezonabilă și mai sigură este să se considere că AL numește în funcția de RPD acele persoane **care sunt responsabile cu toate activitățile de prelucrare a datelor** din cadrul organizației (relațiile cu cetățenii, angajații, candidații pentru posturile vacante, foștii angajați, alte autorități publice etc.).

2.1.2. Activitățile principale ale operatorului sau ale persoanei împuternicite de operator […] necesită o monitorizare periodică și sistematică a persoanelor vizate pe scară largă

Activitățile de prelucrare a datelor din cadrul AL intră, în general, în domeniul de aplicare al punctului 2.1.1. de mai sus, adică AL ar trebui să numească RPD în baza capacității sale de autoritate / organism public. Pentru mai multă claritate, mai jos va fi făcută o scurtă analiză a celorlalte două situații precizate în RGPD de numire obligatorie a RPD. Informațiile sunt relevante pentru entitățile private al căror capital se află în proprietatea parțială sau totală a municipalității sau a altor AL / organisme de stat, care nu intră sub incidența „autorității / organismului public”.

Termenul **„activități principale”** se referă la operațiunile cheie necesare pentru atingerea obiectivelor operatorului sau persoanei împuternicite de operator[iii]. Exemplele oferite de WP29 includ prelucrarea înregistrărilor medicale realizate în spitale și supravegherile efectuate de companiile de securitate private. Pe de altă parte, activitățile standard de suport IT ale angajaților nu fac parte din „activitatea principală” a organizației[iv].

Conceptul de **„scară largă”** nu primește o definiție explicită în RGPD. Se menționează numai că prelucrarea la nivel regional, național sau supranațional, care cuprinde un volum considerabil de date ce ar putea să afecteze un număr mare de persoane vizate și care sunt susceptibile să creeze un risc ridicat, pote fi considerată pe scară largă. Cabinetele individuale de avocatură sau asistență medicală nu prelucrează date cu caracter personal pe o scară largă.

WP29 enumeră o serie neexhaustivă de activități ce pot fi considerate prelucrări pe scară largă:

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

- prelucrarea datelor pacientului de către un spital;
- prelucrarea datelor de călătorie ale persoanelor care utilizează sistemul de transport public al orașului (de exemplu, urmărirea prin intermediul cardurilor de călătorie);
- prelucrarea în timp real a datelor geografice ale clienților unui lanț internațional de fast-food în scopuri statistice de către un operator specializat în furnizarea acestor servicii;
- prelucrarea datelor clienților de către o companie de asigurări / bancă;
- prelucrarea datelor personale în scopuri publicitare de către un motor de căutare;
- prelucrarea datelor (conținut, trafic, locație) de către furnizorii de servicii de telefonie mobilă și internet[v].

Termenul **"periodic"** este corelat cu prelucrarea care se petrece permanent (constant) sau în mod regulat. **"Monitorizarea sistematică"** necesită ca prelucrarea să se desfășoare după un anumit plan, strategie sau metodologie similară predefinită, într-o manieră organizată, în cadrul unui sistem[vi]. Exemplele includ, printre altele, operatorii rețelelor de telecomunicații, crearea de profiluri, publicitatea bazată pe analiza comportamentală a consumatorului, dispozitivele inteligente etc.

2.1.3. Activitățile principale ale operatorului sau ale persoanei împuternicite de operator constau în prelucrarea pe scară largă a unor categorii speciale de date […] sau a unor date cu caracter personal privind condamnări penale și infracțiuni

Pentru termenii „activități principale" și „scară largă", a se vedea punctul 2.1.2 de mai sus.

Orice prelucrare pe scară largă care face parte din activitatea principală a organizației și care vizează **fie** categorii speciale de date, **fie** date personale privind condamnări penale și infracțiuni ar trebui să impună desemnarea RPD.

Din categoriile speciale de date fac parte:

- datele persoanle care dezvăluie originea rasială sau etnică;
- opiniile politice;
- credințele religioase sau convingerile filosofice;
- apartenența sindicală;
- caracteristicile genetice;
- datele biometrice pentru identificarea unică a unei persoane fizice;
- datele cu privire la starea de sănătate sau orientarea sexuală.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

Datele personale privind condamnările penale și infracțiunile pot include informații care se regăsesc în hotărârile judecătorești, cazierele judiciare, documentele organelor de anchetă.

2.2. Alte situații de numire a RPD

2.2.1. Numirea obligatorie în conformitate cu dreptul Uniunii sau cu dreptul intern

Confrom articolului 37, alineatul (4) din RGPD, UE și / sau statele membre au dreptul să prevadă alte situații în care numirea RPD este obligatorie. Asemenea numiri pot fi impuse pe bază calitativă (cum este cazul activităților de prelucrare specifice unui anumit sector) sau cantitativă (în cazul în care organizația prelucrează datele personale ale unui anumit număr de persoane vizate). De exemplu, Germania a introdus în legislația sa cerințe mai permisive decât ale RGPD: (i) societățile care desfășoară activități pe teritoriul său și care angajează cel puțin 10 persoane pentru prelucrarea automatizată a datelor sunt obligate să numească un RPD; (ii) dacă prelucrarea automatizată se efectuează în scopul unui transfer cu date la vedere, al unui transfer anonim, sau pentru analize de piață sau de opinie, societățile trebuie să numească un RPD indiferent de numărul angajaților responsabili cu prelucrarea[vii].

2.2.2. Numirea voluntară

RGPD permite și numirea volutară a RPD. O astfel de abordare este oportună pentru organizațiile care își propun să demonstreze respectarea normelor privind protecția datelor sau să promoveze transparența și încrederea. Întrucât activitatea AL se află mai curând sub incidența cerinței numirii obligatorii, numirea voluntară este valabilă pentru organizațiile al căror capital este deținut de municipalitate / stat – de exemplu, întreprinderile de transport public, școlile / universitățile de stat, frunizorii publici de utilități (apă, gaz, electricitate) etc.

2.3. Relațiile contractuale cu RPD

2.3.1. Contractul de muncă

RGPD prevede explicit posibilitatea desemnării RPD în baza unui contract de muncă. Aceasta implică: (i) numirea unei persoane care lucrează deja în cadrul organizației pentru a-și combina funcția cu funcțiile RPD sau (ii) crearea unui nou post pentru RPD. Alegerea între cele două variante depinde în mare măsură de structura, numărul angajaților, volumul de muncă, tipul și numărul activităților de prelucrare a datelor, și ar trebui să se facă de la caz la caz. Dacă AL este suficient de mică (de pildă, este situată într-un sat cu puțini locuitori), este rezonabil să nu fie numit un nou angajat, ci funcția de RPD să fie preluată de cineva care lucrează deja în organizație – cu condiția evitării conflictului de interese. Dimpotrivă, dacă AL este mare și / sau zilnic în cadrul său este

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

prelucrat un volum semnificativ de date cu caracter personal (sau date sensibile, date privind condamnări penale și infracțiuni), atunci decizia creării unei noi poziții (cel puțin) de RPD pare justificată.

2.3.2. Contractul de servicii

RGPD nu obligă organizațiile să desemneze RPD numai din rândul presonalului. Regulamentul prevede că funcția RPD poate fi externalizată unei persoane / organizații externe în baza unui contract de servicii. WP29 recomandă ca bună practică pentru echipele de RPD externalizate să specifice în clauzele contractului o persoană cu rol de conducere și persoanele responsabile cu fiecare client[viii]. În plus, fiecare membru RPD al organizației externalizate trebuie să îndeplinească toate cerințele impuse de RGPD.

Totodată, externalizarea funcțiilor RPD este indicată, deoarece organizațiile care nu fac parte din AL pot să posede nivelul necesar de cunoștințe de specialitate, experiența relevantă și certificările corespunzătoare[ix].

Nu în ultimul rând, în funcție de legislația locală, încheierea unui contract de servicii cu un RPD extern poate presupune efectuarea unor proceduri formale (de exemplu, în temeiul legislației privind achizițiile publice).

3. FUNCȚIA RPD

3.1. Implicarea în toate chestiunile legate de protecția datelor cu caracter personal

RGPD prevede că RPD ar trebui să se ocupe cu tot ce ține de protecția datelor cu caracter personal în cadrul organizației. WP29 vede în implicarea RPD (prin consultări, avize, control etc.) în fiecare proces unul din instrumentele pentru asigurarea confidențialității[x].

În practică, implicarea RPD în cadrul organizației ar putea avea următoarele consecințe:

- Solicitarea de avize de către operator în timpul realizării unei evaluări a impactului asupra protecției datelor (EIPD) – conform articolului 35, alineatul 2 din RGPD;
- Participarea la întâniri de lucru (WP29 recomandă participarea la întâlnirile de management de nivel înalt și mediu, însă în practică interacțiunea RPD cu experții poate avea o valoare adăugată similară și chiar mai mare);
- Consultarea RPD de fiecare dată când trebuie luată o decizie managerială referitoare la prelucrarea datelor;
- Consultarea RPD ori de câte ori se produc încălcări ale securității datelor cu caracter personal.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

3.2. Asigurarea resurselor necesare și a independenței

RPD nu și-ar putea îndeplini funcția dacă nu ar dispune de resurse. În acest sens, managementul organizației este responsabil cu garantarea acestora, cel puțin în ceea ce privește:

- **Aspectele organizaționale**
  - RPD ar trebui să dispună de o echipă care să îi sprijine în îndeplinirea funcțiilor. Acest lucru este extrem de important pentru organizațiile mai mari. În anumite cazuri soluția ar putea să fie chiar numirea mai multor RPD.
  - Accesul la toate celelalte echipe din cadrul organizației. RPD nu și-ar putea exercita în mod corespunzător funcțiile dacă nu ar interacționa cu toate echipele responsabile cu prelucrarea datelor (de exemplu, registratura, contabilitatea, departamentul juridic, IT sau cel de resurse umane);
  - RPD ar trebui să răspundă numai în fața conducerii de la nivel înalt. RGPD prevede explicit acest lucru. În contextul AL pot fi avuți în vedere: primarul, consiliul municipal, directorul / președintele unității administrative etc. Această cerință este foarte importantă pentru asigurarea independenței RPD. În cazul în care relația dintre RPD și management ar fi indirectă (prin intermediari precum șeful departamentului juridic sau al departamentului de resurse umane), RPD nu și-ar putea îndeplini în mod adecvat funcțiile, deoarece s-ar afla în situația de a răspunde în fața cuiva asupra căruia ar trebui să își exercite controlul.
  - Timp pentru îndeplinirea funcției. Această cerință ar trebui respectată în special în cazurile în care RPD este desemnat cu fracțiune de normă sau atunci când RPD externalizat realizează și alte sarcini pe lângă protecția datelor[xi]. WP29 recomandă ca o bună practică alocarea unui procent de timp pentru funcția RPD, în cazul în care aceasta nu este realizată cu normă întreagă.
- **Aspectele financiare**
  - RPD ar trebui să dispună de resurse financiare pentru exercitarea funcției. Dacă organizația nu asigură un buget suficient pentru activitățile de protecție a datelor, exercitarea adecvată a funcției RPD ar putea fi pusă în pericol.
  - RPD ar trebui să dispună de facilități și echipamente (încăperi, calculatoare, conexiuni la internet, soluții tehnice precum programe software etc.).
- **Aspectele educaționale** – nivelul cunoștințelor de specialitate al RPD ar trebui actualizat constant (prin cursuri, acces la literatura recentă etc.). Având în vedere că protecția datelor reprezintă o arie foarte dinamică a cunoașterii umane, este de

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

înțeles că RPD ar trebui să fie pus la curent cu ultimele tendințe și evoluții ale domeniului pentru a putea asigura în cadrul organizației cel mai înalt nivel de protecție a datelor și pentru a putea răspunde noilor provocări venite din direcția dezvoltării tehnologice și juridice.

Un aspect important al independenței RPD este **interzicerea sancționării / provocării unor consecințe nefavorabile** acestora pentru îndeplinirea sarcinilor. Consecințele nefavorabile ar putea varia în funcție de o gamă largă de situații – de la concediere sau alte sancțiuni disciplinare până la refuzul promovării sau acordării de beneficii pe care ceilalți angajați le primesc etc. Poate fi de așteptat ca statele membre să își modifice legislația muncii și să prevadă protejarea RPD împotriva concedierii pe perioada în care își exercită funcțiile și pe o perioadă ulterioară[xii]. În același timp, ar trebui făcută o interpolare rezonabilă la această înterdicție – RPD să nu poată fi sancționați pentru executarea corespunzătoare a serviciilor. Cu toate acestea, în cazul în care RPD nu dispun de cunoștințele și abilitățile necesare, provoacă încălcări disciplinare etc., organizațiile ar trebui să îi poată respinge pe baza tuturor motivelor de concediere disponibile în legislația muncii.

3.3. Conflictul de interese

Dacă RPD este desemnat în baza unui contract de muncă, această desemnare nu trebuie să conducă la conflicte de interese. Conflictul de interese ar putea să apară dacă RPD ocupă o altă funcție în cadrul organizației, care determină mijloacele și scopurile prelucrării datelor. Altfel spus, RPD nu poate fi în același timp director, director executiv, director financiar, contabil șef, director medical, șef al departamentului de marketing, resurse umane sau IT[xiii]. Conflictele de interese pot fi provocate și de rolurile inferioare din structura organizatorică, dacă asemenea poziții presupun determinarea mijloacelor și scopurilor prelucrării (de exemplu, contabil, consilier juridic, specialist IT).

Conflictul de interese poate apărea nu numai în cazul desemnării RPD în baza unui contract de muncă, ci și în cazul RPD externalizat. În cazul în care RPD-ului i se solicită să reprezinte în fața instanțelor de judecată operatorii sau persoanele împuternicite de operatori pentru probleme legate de protecția datelor, ia naștere un conflict de interese, întrucât operatorul și persoana împuternicită au interese contrare.

4. SARCINILE RPD

4.1. Monitorizarea

Una dintre sarcinile principale ale RPD este monitorizarea tuturor activităților de prelucrare a datelor din cadrul organizației. Aceasta se află într-o strânsă legătură cu

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

colectarea informațiilor, analizarea acestora, formularea de clarificări, recomandări și acordarea avizelor. Sarcina monitorizării se concentrează asupra proceselor interne din cadrul organizației, astfel încât ar trebui să fie informate și consiliate la nivel de experți nu numai persoanele aflate la conducere, ci și angajații obișnuiți ale căror atribuții sunt legate de prelucrarea datelor cu caracter personal.

4.2. EIPD

RGPD prevede că RPD ar trebui să se implice în evaluarea impactului asupra protecției datelor, adoptând un rol de consiliere. WP29 recomandă ca o bună practică solicitarea de consultanță din partea RPD cu privire la unul sau mai multe dintre următoarele aspecte:

- dacă EIPD ar trebui realizată;
- ce metodologie ar trebui urmată pentru realizarea EIPD;
- dacă EIPD va fi efectuată intern sau externalizată;
- ce măsuri de siguranță (inclusiv măsuri tehnice și organizatorice) să fie aplicate pentru a elimina orice riscuri la adresa drepturilor și intereselor persoanelor vizate;
- dacă EIPD a fost corect efectuată, iar conluziile sale sunt în conformitate cu RGPD[xiv].

Dacă managementul organizației decide să se abată de la recomandările RPD, este indicat, în virtutea principiului responsabilității, ca decizia respectivă și motivele care au stat la baza sa să fie documentate, astfel încât să poată fi prezentate autorităților de supraveghere în cazul unui audit.

4.3. Punctul de contact

RPD reprezintă principalul punct de contact atât pentru autoritățile de supraveghere (articolul 39, alineatul (1), punctul (e) din RGPD), cât și pentru persoanele vizate (articolul 38, alineatul (4) din RGPD) în orice chestiune privind protecția datelor de la nivelul organizației. Prin urmare, este extrem de important să fie comunicate în mod corespunzător detaliile de contact ale RPD autorității de supraveghere și persoanelor vizate. Mai mult decât atât, cerința furnizării datelor de contact ale RPD constituie unul dintre elementele principiului transparenței – conform articolelor 12, 13 și 14 ale RGPD.

Nimic din RGPD nu exclude posibilitatea de a solicita consiliere din partea autorităților de supraveghere cu privire la orice chestiune legată de protecția datelor în cadrul organizației.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

4.4. Păstrarea evidenței

Deși obligația de a păstra evidența actvităților de prelucrare nu cade în sarcina RPD ci a operatorilor și a persoanelor împuternicite de operatori, nimic din RGPD nu împiedică organizațiile să atribuie această funcție și RPD. Sarcinile RPD enumerate în RGPD reprezintă un **set minim**, astfel încât organizațiile sunt libere să delege orice altă sarcină pentru RPD. WP29 consideră însărcinarea RPD cu obligația păstrării înregistrărilor efectuate drept unul dintre instrumentele care permit RPD să își îndeplinească în mod corespunzător sarcinile de monitorizare, informare și consiliere a operatorilor / persoanelor împuternicite de operatori[xv]. Dat fiind faptul că înregistrarea este un instrument eficient pentru păstrarea evidențelor, este oportună delegarea acestei obligații către RPD.

5. CONCLUZIE ȘI RECOMANDĂRI

RPD reprezintă una dintre figurile-cheie în asigurarea respectării noilor norme privind protecția datelor. Importanța acestui rol depinde în mare măsură de organizația în sine. Dacă organizația implică în mod adecvat RPD în toate chestiunile legate de protecția datelor și îi asigură acestuia resursele necesare pentru îndeplinirea funcției, atunci RPD poate fi unul dintre factorii decisivi în asigurarea conformității și creșterea nivelului de încredere socială. În caz contrar, RPD devine o figură iluzorie, fără o altă funcție reală decât, eventual, gestionarea comunicării legate de protecția datelor, ceea ce nu este tocmai ideea rolului stabilit în cadrul RGPD.

AL sunt încurajate să desemneze RPD calificați, ceea ce se poate dovedi o sarcină dificilă, având în vedere lipsa de pregătire a indivizilor la nivelul UE. În orice caz, următorii ani vor determina cum va evolua rolul RPD. Oricum ar sta lucrurile, este în beneficiul societății ca AL să poată oferi exemple de pionierat în ceea ce privește cea mai bună întrebuințare a figurii RPD.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

6. BIBLIOGRAFIE

Cărți

- **Harting, N.** Datenschutz-Grundverordnung: Das neue Datenschutzrecht in der betrieblichen Praxis, Verlag Dr. Otto Schmidt KG, Köln, 2016;
- **Voigt, P., von dem Bussche, A.** The EU General Data Protection Regulation (GDPR) – A Practical Guide, Springer International Publishing (2017);
- **Boardman, R., Mullock, J., Mole, A.** Bird & Bird Guide to General Data Protection Regulation (2016);
- **EU** General Data Protection Regulation (GDPR). An Implementation and Compliance Guide, IT Governance Publishing, Cambridgeshire (2016);

Documente referitoare la Grupul de lucru ”Articolul 29”

- WP29, Guidelines on Data Protection Officers (‘DPOs’), WP 243 rev.01;

Link-uri web

- http://europa.eu/rapid/press-release_IP-18-386_en.htm
- https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en

7. NOTE

[i] WP29, Guidelines on Data Protection Officers (‘DPOs’), WP 243 rev.01, p. 6.
[ii] Ibid.
[iii] Ibid.
[iv] Ibid, p. 6-7.
[v] Ibid, p. 8.
[vi] Vezi interpretarea exactă a grupului de lucru al articolului 29 în WP29, Guidelines on Data Protection Officers (‘DPOs’), WP 243 rev.01, p. 8.
[vii] Demmel, A. The New German Federal Data Protection Act, Squire Patton Boggs, URL: <https://www.squirepattonboggs.com/~/media/files/insights/publications/2017/09/the-new-german-federal-data-protection-act/27836--german-federal-data-protection-alert.pdf> (26.03.2018);
[viii] WP29, Guidelines on Data Protection Officers (‘DPOs’), WP 243 rev.01, p. 22-23.
[ix] EU General Data Protection Regulation (GDPR). An Implementation and Compliance Guide, IT Governance Publishing, Cambridgeshire (2016), p. 58.
[x] WP29, Guidelines on Data Protection Officers (‘DPOs’), WP 243 rev.01, p. 13.
[xi] Ibid, p. 14.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

[xii] Germania a introdus deja protecția RPD împotriva concedierii sau la un an după încetarea numirii, cu excepția unor motive de reziliere extraordinară. A se vedea în acest sens, Demmel, A. The New German Federal Data Protection Act, Squire Patton Boggs, URL: <https://www.squirepattonboggs.com/~/media/files/insights/publications/2017/09/the-new-german-federal-data-protection-act/27836--german-federal-data-protection-alert.pdf> (26.03.2018);
[xiii] WP29, Guidelines on Data Protection Officers ('DPOs'), WP 243 rev.01, p. 16.
[xiv] Ibid, p.17.
[xv] WP29, Guidelines on Data Protection Officers ('DPOs'), WP 243 rev.01, p. 19.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

ProLegis

Evaluarea Impactului asupra Protecției Datelor

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

ProLegis

Cuprins

1. Cadru legal 4

1.1. Regulamentul general privind protecția datelor (RGPD) 4

2. Când este necesară EIPD? 7

2.1. Elemente de bază 7

2.2. Cazuri în care EIPD este obligatorie 7

2.2.1. Considerații suplimentare privind necesitatea efectuării unei EIPD 8

2.2.2. Realizarea unei EIPD pentru mai multe sisteme similare de prelucrare a datelor 8

2.2.3. Liste pozitive și negative pentru EIPD 9

2.3. Calendarul EIPD 9

2.4. Revizuirea EIPD 10

2.5. Consultarea cu Autoritatea pentru Protecția Datelor în temeiul articolului 36 din RGPD 10

3. Cine este responsabil pentru efectuarea unei EIPD? 11

3.1. Elemente de bază 11

3.2. Participarea la EIPD 11

4. Cum se efectuează EIPD 12

4.1. Elemente de bază 12

4.2. Implementarea unei EIPD 12

4.3. Conținutul minim al EIPD 12

4.4. Procesul EIPD 13

4.5. Includerea persoanelor vizate sau a reprezentanților acestora 15

4.6. Raportul implementării unei evaluări a impactului asupra confidențialității 16

5. Concluzii și recomandări 18

6. Bibliografie 20

6.1. Cărți și articole 20

6.2. Documente referitoare la Grupul de lucru ”Articolul 29” 20

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

6.3. Link-uri Web 20

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

1. Cadru legal

1.1. Regulamentul general privind protecția datelor (RGPD)

Articolul 35

Evaluarea impactului asupra protecției datelor

(1) Având în vedere natura, domeniul de aplicare, contextul și scopurile prelucrării, în cazul în care un tip de prelucrare, în special cel bazat pe utilizarea noilor tehnologii, este susceptibil să genereze un risc ridicat pentru drepturile și libertățile persoanelor fizice, operatorul efectuează, înaintea prelucrării, o evaluare a impactului operațiunilor de prelucrare prevăzute asupra protecției datelor cu caracter personal. O evaluare unică poate aborda un set de operațiuni de prelucrare similare care prezintă riscuri ridicate similare.

(2) La realizarea unei evaluări a impactului asupra protecției datelor, operatorul solicită avizul responsabilului cu protecția datelor, dacă acesta a fost desemnat.

(3) Evaluarea impactului asupra protecției datelor menționată la alineatul (1) se impune mai ales în cazul:

(a) unei evaluări sistematice și cuprinzătoare a aspectelor personale referitoare la persoane fizice, care se bazează pe prelucrarea automată, inclusiv crearea de profiluri, și care stă la baza unor decizii care produc efecte juridice privind persoana fizică sau care o afectează în mod similar într-o măsură semnificativă;

(b) prelucrării pe scară largă a unor categorii speciale de date, menționată la articolul 9 alineatul (1), sau a unor date cu caracter personal privind condamnări penale și infracțiuni, menționată la articolul 10; sau

(c) unei monitorizări sistematice pe scară largă a unei zone accesibile publicului.

(4) Autoritatea de supraveghere întocmește și publică o listă a tipurilor de operațiuni de prelucrare care fac obiectul cerinței de efectuare a unei evaluări a impactului asupra protecției datelor, în conformitate cu alineatul (1). Autoritatea de supraveghere comunică aceste liste comitetului menționat la articolul 68.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

(5) Autoritatea de supraveghere poate, de asemenea, să stabilească și să pună la dispoziția publicului o listă a tipurilor de operațiuni de prelucrare pentru care nu este necesară o evaluare a impactului asupra protecției datelor. Autoritatea de supraveghere comunică aceste liste comitetului.

(6) Înainte de adoptarea listelor menționate la alineatele (4) și (5), autoritatea de supraveghere competentă aplică mecanismul pentru asigurarea coerenței menționat la articolul 63 în cazul în care aceste liste implică activități de prelucrare care presupun furnizarea de bunuri sau prestarea de servicii către persoane vizate sau monitorizarea comportamentului acestora în mai multe state membre ori care pot afecta în mod substanțial libera circulație a datelor cu caracter personal în cadrul Uniunii.

(7) Evaluarea conține cel puțin:

(a) o descriere sistematică a operațiunilor de prelucrare preconizate și a scopurilor prelucrării, inclusiv, după caz, interesul legitim urmărit de operator;

(b) o evaluare a necesității și proporționalității operațiunilor de prelucrare în legătură cu aceste scopuri;

(c) o evaluare a riscurilor pentru drepturile și libertățile persoanelor vizate menționate la alineatul (1); și

(d) măsurile preconizate în vederea abordării riscurilor, inclusiv garanțiile, măsurile de securitate și mecanismele menite să asigure protecția datelor cu caracter personal și să demonstreze conformitatea cu dispozițiile prezentului regulament, luând în considerare drepturile și interesele legitime ale persoanelor vizate și ale altor persoane interesate.

(8) La evaluarea impactului operațiunilor de prelucrare efectuate de operatorii sau de persoanele împuternicite de operatori relevante, se are în vedere în mod corespunzător respectarea de către operatorii sau persoanele împuternicite respective a codurilor de conduită aprobate menționate la articolul 40, în special în vederea unei evaluări a impactului asupra protecției datelor.

(9) Operatorul solicită, acolo unde este cazul, avizul persoanelor vizate sau al reprezentanților acestora privind prelucrarea prevăzută, fără a aduce atingere protecției intereselor comerciale sau publice ori securității operațiunilor de prelucrare.

(10) Atunci când prelucrarea în temeiul articolului 6 alineatul (1) litera (c) sau (e) are un temei juridic în dreptul Uniunii sau al unui stat membru sub incidența căruia intră operatorul, iar dreptul respectiv reglementează operațiunea de prelucrare specifică sau

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

setul de operațiuni specifice în cauză și deja s-a efectuat o evaluare a impactului asupra protecției datelor ca parte a unei evaluări a impactului generale în contextul adoptării respectivului temei juridic, alineatele (1)-(7) nu se aplică, cu excepția cazului în care statele membre consideră că este necesară efectuarea unei astfel de evaluări înaintea desfășurării activităților de prelucrare.

(11) Acolo unde este necesar, operatorul efectuează o analiză pentru a evalua dacă prelucrarea are loc în conformitate cu evaluarea impactului asupra protecției datelor, cel puțin atunci când are loc o modificare a riscului reprezentat de operațiunile de prelucrare.

Considerentele 89-96:

Articolul 35 al RGPD este corelat cu articolele 24, 25 și 32.

Principala deosebire dintre articolul 32 (Securitatea prelucrării) și articolul 35 (Evaluarea impactului asupra protecției datelor - EIPD) este că primul vizează riscurile legate de prejudicii precum atacurile, în timp ce al doilea **se concentrază cu precădere asupra riscurilor apărute ca urmare a prelucrării obișnuite a datelor.** EIPD este un instrument important pentru implementarea protecției datelor prin mijloace tehnologice (protecția datelor începând cu momentul conceperii), astfel cum se prevede la articolul 25, alineatul 1. Ambele articole se bazează pe principiul precauției, și anume identificarea riscurilor deja existente în fazele inițiale de proiectare, pentru a lua în considerare măsurile de contracarare relevante, înainte ca orice sistem de prelucrare a datelor să fie pus în aplicare și să devină operațional.

EIPD este un instrument de identificare și analizare a unor astfel de riscuri. În situațiile în care EIPD nu este obligatorie, o analiză a riscurilor asociate este totuși necesară, pentru a pune în aplicare în mod adecvat articolul 25 și articolul 32. Ambele prevederi se referă la drepturile și libertățile persoanelor fizice. Profunzimea și documentația necesară a analizei de risc depind de complexitatea și gradul de risc al prelucrării. Recomandarea noastră este furnizați o documentație scrisă a analizei riscurilor.

Implementarea principului protecției datelor începând cu momentul conceperii depășește riscruile implementate în prealabil într-o analiză de ultimă oră și cuprinde decizii luate ad-hoc de către dezvoltatorii de sisteme (ingineria de confidențialitate) atunci când se aplică principiile de minimizare a datelor.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

2. Când este necesară EIPD?[1]

2.1. Elemente de bază

O EIPD trebuie efectuată înainte de prelucrarea datelor cu caracter personal care prezintă un grad de risc ridicat pentru drepturile și libertățile persoanelor fizice.

În principiu, EIPD trebuie efectuată pentru orice formă de prelucrare a datelor, cu excepția cazului în care se poate determina dinainte că drepturile și libertățile persoanelor fizice nu sunt afectate de o anumită operațiune de prelucrare.

Punctele enumerate la articolul 35, alineatul (3), sau la considerentul 91 prevăd pentru ce tip de prelucrare a datelor trebuie luat în considerare un astfel de risc. Accentul se pune pe utilizarea așa-numitelor tehnologii noi, un concept juridic vag, introdus în RGPD cu referire la EIPD. O evaluare a riscurilor trebuie să ia în considerare nu numai constelațiile de risc existente, ci și probabilitatea evenimentelor viitoare, astfel încât să poată fi realizată o prognoză a acestora. Rezultatele evaluării trebuie să fie documentate.

Articolul 35, alineatul (1), ultimul enunț, coroborat cu considerentul 92 oferă un punct de vedere important pentru necesitatea efectuării unei EIPD: „În anumite circumstanțe, poate fi rezonabil și adecvat din punct de vedere economic să nu se aplice o evaluare a impactului asupra confidențialității numai pentru un proiect special, ci să fie lărgit domeniul de aplicare tematic. De exemplu, atunci când autoritățile sau alte organisme publice doresc să creeze o platformă comună de aplicare sau prelucrare sau când mai multe părți interesate doresc să implementeze un mediu comun de aplicare sau prelucrare pentru un întreg sector de afaceri, segment de piață sau activitate orizontală larg răspândită”.

2.2. Cazuri în care EIPD este obligatorie

Articolul 35, alineatul (3) stabilește că EIPD se impune în cazul:

(a) unei evaluări sistematice și cuprinzătoare a aspectelor personale referitoare la persoane fizice, care se bazează pe prelucrarea automată, inclusiv crearea de

[1] Textul care urmează se bazează pe Kastelitz, M., Hötzendorfer, W., Riedl, R., Ausgewählte Fragen der Durchführung einer Datenschutz-Folgenabschätzung gemäß Art 35 DSGVO, Jahrbuch Datenschutzrecht 2017, p113 și urm.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

profiluri, și care stă la baza unor decizii care produc efecte juridice privind persoana fizică sau care o afectează în mod similar într-o măsură semnificativă;

(b) prelucrării pe scară largă a unor categorii speciale de date, menționată la articolul 9 alineatul (1), sau a unor date cu caracter personal privind condamnări penale și infracțiuni, menționată la articolul 10; sau

(c) unei monitorizări sistematice pe scară largă a unei zone accesibile publicului.

2.2.1. Considerații suplimentare privind necesitatea efectuării unei EIPD

Considerentul 91 enumeră și alte cazuri în care EIPD este necesară:

Operațiuni de prelucrare

(a) care implică un număr mare de oameni și/sau un grad ridicat de risc și/sau utilizează tehnologie de ultimă oră la scară largă;

b) care implică un grad ridicat de risc și îngreunează exercitarea drepturilor persoanelor vizate;

(c) în situațiile în care datele cu caracter personal sunt prelucrate în scopul luării de decizii care vizează anumite persoane fizice în urma unei evaluări sistematice și cuprinzătoare a aspectelor personale referitoare la persoane fizice, pe baza creării de profiluri pentru datele respective, sau în urma prelucrării unor categorii speciale de date cu caracter personal, a unor date biometrice sau a unor date privind condamnările penale și infracțiunile sau măsurile de securitate conexe;

(d) care implică un grad ridicat de risc, deoarece împiedică persoanele în cauză să își exercite un drept, să utilizeze un serviciu sau să execute un contract;

(e) care prezintă un gad ridicat de risc, deoarece sunt efectuate în mod sistematic la scară largă.

2.2.2. Realizarea unei EIPD pentru mai multe sisteme similare de prelucrare a datelor

Articolul 35, alineatul (1) prevede că se poate realiza o singură EIPD pentru sisteme de prelucrare cu grad de risc similar. La evaluarea unei asemenea similitudini trebuie luat în considerare scopul general al fiecărui caz de prelucrare a datelor. Considerentul 92 afirmă că, având în vedere costurile economice, EIPD poate avea o sferă de aplicare mai largă, oferind membrilor dintr-un anumit sector industrial sau segment de piață posibilitatea de a acoperi aplicații, medii de procesare sau practici orizontale larg împărtășite cu o singură aplicare de EIPD.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

2.2.3. Liste pozitive și negative pentru EIPD

Se poate presupune că agențiile de reglementare vor publica liste pozitive/negative în scopul înlesnirii deciziei cu privire la necesitatea realizării EIPD într-un anumit caz. Aceste liste vor defini tipurile de prelucrare care necesită EIPD („listele pozitive") și cazurile în care nu este necesară EIPD („listele negative"). Ambele liste trebuie transmise de organismele naționale de reglementare Comitetului european pentru protecția datelor, ca parte a regimului de coerență a reglementărilor (articolul 35, alineatul 4), pentru a asigura o mai bună armonizare în întreaga UE.

Trebuie menționat faptul că Grupul de lucru "Articolul 29" (WP29) recomandă efectuarea unei EIPD și în cazul în care nu este suficient de clar dacă aceasta este necesară, pentru a contribui la îndeplinirea cerințelor legale pentru protecția adecvată a datelor.

2.3. Calendarul EIPD

Calendarul și metoda EIPD trebuie să fie determinate de operator. Sunt prevăzute sancțiuni juridice pentru nerealizarea EIPD. Se recomandă începerea pregătirii EIPD încă din primele etape ale unui proiect. Fiecare departament sau personalul avizat implicat în prelucrarea datelor trebuie să inițieze procesele relevante. Se recomandă instruirea pentru a crește gradul de conștientizare cu privire la nevoia EIPD în cadrul organizației.

Luarea în considerare a măsurilor de minimizare a riscurilor în stadiul incipient al oricărui proiect care implică prelucrarea datelor poate contribui la menținerea eforturilor birocratice la un nivel relativ scăzut.

EIPD poate ghida căutarea de soluții adecvate și poate contribui la implementarea eficientă și în timp util a cerințelor cu privire la protecția datelor prin intermediul soluțiilor tehnologice adecvate (protecția datelor începând cu momentul conceperii), precum și la alegerea setărilor implicite.

În cazul pregătirilor cuprinzătoare și intensive, EIPD va ghida un proiect din stadiul incipient și până la implementarea operațională finală, demonstrând caracterul iterativ al procesului EIPD.

Rămâne o întrebare deschisă dacă EIPD este necesară și pentru prelucrarea activităților aflate în desfășurare înainte de intrarea în vigoare a RGPD (25 mai 2018). În mod normal, EIPD este necesară numai pentru procesele care devin operaționale după 25 mai 2018 sau care suferă modificări semnificative după această dată.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

Întrucât în aceste cazuri sistemul de prelucrare a datelor este deja operațional, nu este posibilă o verificare prealabilă. Mai mult decât atât, aceste operațiuni nu există într-un spațiu nereglementat (presupunând că au fost luate în considerare toate reglementările legale și cerințele de raportare ale cadrului juridic anterior).

Cu toate acestea, WP29 recomandă cu fermitate efectuarea EIPD pentru sistemele de prelucrare deja utilizate pentru a evita incertitudinile juridice și chiar sancțiunile legale.

2.4. Revizuirea EIPD

După efectuarea unei EIPD trebuie revizuită implementarea măsurilor sugerate, iar dacă este cazul, poate fi necesară o revizuire chiar a prelucrării datelor, pentru a identifica orice noi elemente de risc. Considerentul 89 prevede că ar putea fi nevoie de o revizuire a EIPD în timp util, după o primă evaluare. Atunci când se efectuează o EIPD, un interval de timp pentru verificări de rutină sau pentru ajustări viitoare ar trebui să facă parte din documentație.

Ar trebui luate în considerare evoluțiile tehnologice, noile reglementări juridice și schimbările în rutinele de prelucrare. În cazul în care se materializează un risc, trebuie efectuată o nouă EIPD.

Obligația efectuării unei EIPD îi revine operatorului de date, care se ocupă de documentație. Documentația și rapoartele nu trebuie să conțină numai informații despre EIPD realizată, ci și să prezinte motivele pentru care nu a fost efectuată o EIPD completă sau motivele pentru încheierea unei EIPD după identificarea unor riscuri ridicate pentru persoanele vizate.

2.5. Consultarea cu Autoritatea pentru Protecția Datelor în temeiul articolului 36 din RGPD

Operatorul de date trebuie să se consulte cu Autoritatea pentru Protecția Datelor (APD) în cazul în care EIPD prezintă riscuri majore, iar operatorul nu știe ce măsuri de remediere să ia pentru atenuarea unor astfel de riscuri. APD are obligația să răspundă acestei solicitări de consultare în termen de paisprezece săptămâni. Pentru proiectele complexe și inovatoare, se recomandă inițierea unei EIPD cât mai curând posibil, astfel încât orice recomandare din partea APD să poată fi luată în considerare pe durata implementării.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

3. Cine este responsabil pentru efectuarea unei EIPD?

3.1. Elemente de bază

Responsabilitatea efectuării unei EIPD îi aparține operatorului – în acest caz autoritatea publică locală. Inițial, Comisia Europeană a propus să atribuie această responsabilitate persoanei împuternicite de operator. În schimb, considerentul 95 afirmă că persoana împuternicită sprijină operatorul, atunci când este necesar sau la cerere, pentru a asigura respectarea obligațiilor ce decurg din evaluarea impactului asupra protecției datelor.

În practică, este, prin urmare, adecvat să fie încheiat un contract cu o persoană împuternicită de operator, dacă este disponibilă și a fost deja selectată, pentru a se implica și a acorda sprijin activ pe parcursul întregii EIPD. Acest lucru este în afara articolului 28, alineatul (3), litera (f), care prevede ca respectivul contract (sau orice alt instrument juridic) să stipuleze că persoana împuternicită de operator îl ajută pe acesta să asigure respectarea obligațiilor prevăzute la articolele 32-36, ținând seama de caracterul prelucrării și informațiile aflate la dispoziția persoanei împuternicite. Deseori, numai persoana împuternicită de operator dispune de informațiile necesare pentru evaluarea aspectelor legate de prelucrare. În acest sens, trebuie luat în calcul riscul de divulgare a secretelor comericale și de afaceri. Din nou, se recomandă o reglementare contractuală corespunzătoare. Dacă este prevăzută prelucrarea datelor de către operatori comuni, EIPD, în sensul articolului 35, alineatele (1) și (2), poate fi efectuată de unul dintre operatori – ceea ce nu îi scutește de responsabilități pe ceilalți.

3.2. Participarea la EIPD

EIPD ar trebui organizată ca un proiect și, ca atare, să fie echipată cu resurse materiale și umane printr-un nivel ridicat corespunzător de management. La alcătuirea echipei de proiect trebuie să se acorde o atenție deosebită complexității proiectului, cunoștințelor de specialitate și ale celor specifice proiectului și mediului său. În practică, poate fi creată o echipă formată din avocați, personal IT, CISCO, ofițer de protecție a datelor, departamentul care a solicitat prelucrarea („proprietarul datelor”) etc.

O atenție deosebită este acordată asigurării evitării conflictului de interese. Astfel, persoanele care se ocupă de prelucrarea datelor pe viitor nu trebuie să fie considerate independente, pe de altă parte însă, pot oferi o contribuție valoroasă la elaborarea evaluării impactului asupra confidențialității. Implementarea poate fi efectuată de o echipă internă, precum și de terți externi. În mod ideal, ar trebui implicat un organism independent.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

Operatorul solicită avizul responsabilului cu protecția datelor (RPD). În conformitate cu articolul 39, alineatul (1), litera (c), avizul privind EIPD și monitorizarea implementării acesteia se numără printre atribuțiile statutare ale RPD, dar numai la cerere și nu într-o poziție de conducere.

Prin urmare, operatorul are obligația de a obține avizul RPD. Operatorul decide însă când și în ce măsură ar trebui să fie implicat RPD în cadrul procesului. O revizuire ulterioară a raportului final ar fi suficientă. Se recomandă implicarea din timp a responsabilului cu protecția datelor, mai ales datorită competențelor sale.

În funcție de structura organizatorică a operatorului, este indicat ca EIPD să fie aprobată la nivel de conducere sau de un organism autorizat corespunzător.

4. Cum se efectuează EIPD

4.1. Elemente de bază

Trebuie subliniat faptul că RGPD nu prevede nicio formă specifică sau metodă concretă de elaborare a unei evaluări a impactului asupra protecției datelor, care se discută intens la nivel național și european. WP29 afirmă că pot fi utilizate diferite opțiuni de proiectare pentru a sprijini punerea în aplicare a dispozițiilor RGPD și face referire la diverse modele de EIPD (generice sau sectoriale) în Anexa 1.[2]

4.2. Implementarea unei EIPD

Operatorul este, așadar, liber să își aleagă modul de desfășurare a EIPD și îl poate adapta procedurilor interne existente, cu condiția ca autoritatea publică locală să țină seama de cele patru cerințe minime prevăzute în RGPD la articolul 35, alineatul (7), literele (a) - (d), cerințe pe care Grupul de lucru ”Articolul 29” le descrie în detaliu, luând în plus în considerare „implicarea părților interesate” (a se vedea articolul 35, alineatul (2)) și avizul persoanelor vizate (a se vedea articolul 35, alineatul (9)).

4.3. Conținutul minim al EIPD

Articolul 35, alineatul (7), literele (a) - (d) din RGPD, coroborat cu considerentele 84 și 90 impun următorul conținut minim al evaluării:

2 WP29, WP248, 15: Diferite metodologii ar putea fi utilizate pentru a ajuta la punerea în aplicare a cerințelor de bază stabilite în RGPD. A se vedea Anexa 1 pentru exemple de metodologii de evaluare a impactului asupra protecției datelor și confidențialității.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

(a) o descriere sistematică a operațiunilor de prelucrare preconizate și a scopurilor prelucrării, inclusiv, după caz, interesul legitim urmărit de operator;

(b) o evaluare a necesității și proporționalității operațiunilor de prelucrare în legătură cu aceste scopuri;

(c) o evaluare a riscurilor pentru drepturile și libertățile persoanelor vizate menționate la alineatul (1); și

(d) măsurile preconizate în vederea abordării riscurilor, inclusiv garanțiile, măsurile de securitate și mecanismele menite să asigure protecția datelor cu caracter personal și să demonstreze conformitatea cu dispozițiile prezentului regulament, luând în considerare drepturile și interesele legitime ale persoanelor vizate și ale altor persoane interesate.

Literele (c) și (d) sunt manifestări ale așa-numitei abordări bazate pe risc a RGPD, care sunt relevante nu numai pentru implementarea EIPD, ci și în contextul articolelor 24, 25 și 32. Cu alte cuvinte, EIPD este un exemplu specific al abordării bazate pe riscuri a prelucrării datelor, care presupune un grad ridicat de risc pentru drepturile și libertățile persoanelor fizice și solicită, de aceea, un tratament special al riscurilor. În principiu, orice altă verificare a admisibilității privind prelucrarea datelor este inerentă unei evaluări a riscurilor, incluzând măsuri tehnice și organizatorice adecvate de minimizare a riscurilor, înainte de punerea lor în aplicare (a se vedea articolul 24, alineatul (1) din RGPD).

4.4. Procesul EIPD

EIPD ar trebui văzută ca un proces (nu doar un raport), care ar trebui început cât mai curând posibil pentru a influența conceperea subiectului („proiectului"). În consecință, o evaluare a impactului diferă de un audit care evaluează un proiect ex-post și, de obicei, ajunge prea târziu pentru a „tampona" nevoile de protecție a datelor.

În momentul de față există numeroase propuneri pentru implementarea unui proces EIPD, similare cu rezultatele studiului PIAF (2012), care a cartografiat pentru Comisia Europeană metodologiile de evaluare a impactului asupra confidențialității în șapte țări (inclusiv derivarea recomandărilor de bună practică și a elementelor esențiale ale unui proces de evaluare a impactului asupra confidențialității). Au fost identificate următoarele elemente de bază:

1. Determinarea necesității unei evaluări a impactului asupra confidențialității (analiza pragurilor).

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

2. Identificarea echipei de evaluare a impactului asupra confidențialității și stabilirea termenilor de referință.
3. Descrierea proiectului propus (și identificarea părților interesate).
4. Analiza fluxurilor de informații și a altor efecte asupra confidențialității.
5. Consultarea părților interesate.
6. Managementul riscurilor (identificarea riscurilor și a posibilelor soluții).
7. Verificarea conformității juridice.
8. Formularea recomandărilor.
9. Pregătirea și publicarea raportului (de exemplu, pe site-ul organizației).
10. Punerea în aplicare a recomandărilor.
11. Revizuirea și/sau auditul extern(ă) (parte terță).
12. Revizuirea evaluării impactului asupra confidențialității dacă proiectul în cauză se modifică (actualizarea evaluării dacă proiectul suferă modificări).

Modelul EIPD pentru rețelele inteligente și sistemele de contorizare inteligente, menționat explicit în Recomandarea 2014/724/UE a Comisiei Europene, prevede următoarele etape:[3]

1. Etapa 1 – Pre-evaluarea și criteriile care determină necesitatea efectuării unei EIPD.
2. Etapa 2 – Inițierea.
3. Etapa 3 – Identificarea, caracterizarea și descrierea sistemelor/aplicațiilor de rețele inteligente care prelucrează date cu caracter personal.
4. Etapa 4 – Identificarea riscurilor relevante.
5. Etapa 5 – Evaluarea riscurilor de protecție a datelor.
6. Etapa 6 – Identificarea și recomandarea controalelor și a riscurilor reziduale.
7. Etapa 7 – Documentarea și redactarea raportului EIPD.
8. Etapa 8 – Revizuirea și mentenanța.

Noul standard ISO / IEC 29134 oferă îndrumări pentru un proces de realizare a evaluărilor impactului asupra confidențialității și pentru structura și conținutul unui raport EIC. Procesul este împărțit în următoarele patru subprocese:

1. Analiza pragurilor.
2. Pregătirea EIC.
3. Efectuarea EIC.

3 Recomandarea Comisiei 2014/724/UE din 10 octombrie 2014 privind modelul de evaluare a impactului protecției datelor pentru rețele inteligente și sisteme de contorizare inteligente, ABI L 2014/300, 63.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

4. Monitorizarea EIC.

Împărțirea unui proces EIPD este mai degrabă o chestiune de gust, existând propuneri cu trei sau patru etape, până la șase sau șapte etape. Important este însă ca structura procesului să fie inteligibilă și să țină seama în special de cerințele articolului 35, alineatul (7) din RGPD și de recomandările Grupului de lucru ”Articolul 29”.

4.5. Includerea persoanelor vizate sau a reprezentanților acestora

În conformitate cu articolul 35, alineatul (9), operatorul solicită, acolo unde este cazul, avizul persoanelor vizate sau al reprezentanților acestora cu privire la prelucrarea prevăzută, fără a aduce atingere protecției intereselor comerciale sau publice ori securității operațiunilor de prelucrare. Includerea sintagmei „acolo unde este cazul" în contextul negocierilor tripartite face să nu fie clar în ce condiții ar trebui să se obțină în mod concret avizul persoanelor vizate sau al reprezentanților acesteia și în ce cazuri (admisibile) se poate renunța la acest lucru.

Felul în care se solicită avizul este dependent de context, iar WP29 recunoaște diferite moduri de a face acest lucru, cum ar fi realizarea unui studiu (intern sau extern), interviuri formale cu reprezentanți ai personalului sau ai sindicatelor și transmiterea de chestionare către viitorii clienți ai operatorului. Cu toate acestea, operatorul va trebui să se ocupe de avizele persoanelor vizate sau ale reprezentanților acestora și, totodată, să țină cont de ele în evaluarea impactului. În literatura de specialitate este un subiect controversat dacă asociațiile de protecție a consumatorilor pot fi considerate reprezentanți ai persoanelor vizate.[4]

În orice caz, obligația de a consulta *expresis verbis* nu aduce atingere protecției intereselor comerciale sau publice ori securității operațiunilor de prelucrare. Prin urmare, operatorul poate să restricționeze accesul sau chiar să refuze *in extremis* persoanelor vizate sau reprezentanților acestora furnizarea de informații privind prelucrarea. Cel din urmă caz ar face însă imposibilă implicarea în sensul articolului 35, alineatul (9), deoarece existența unor informații suficiente este o condiție *sine qua non* pentru avizul persoanelor vizate sau a reprezentanților acestora.

4 *Martini* in Paal/Pauly (Hrsg), Datenschutz-Grundverordnung (2016) Art 35 Rz 60; dagegen (mangels rechtlicher Verbundenheit) *Laue/Nink/Kremer*, Das neue Datenschutzrecht in der betrieblichen Praxis (2016) 245 Rz 99.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

4.6. Raportul implementării unei evaluări a impactului asupra confidențialității

Trebuie remarcat că raportul EIPD nu reprezintă adevăratul scop al EIPD, ci doar un mijloc de documentare a întregului proces (intern și extern). Raportarea nu trebuie însă subestimată, deoarece documentează implementarea și rezultatele obținute, iar o simplă comunicare de presă trebuie evitată din motive de conformitate. Raportul poate servi și ca ghid sau listă de verificare în desfășurarea EIPD.

În mod surprinzător, articolul 35 al RGPD nu conține nicio cerință explicită cu privire la pregătirea unui raport al desfășurării EIPD. Există, totuși, obligația documentării, ce îi revine operatorului și care rezultă implicit din articolul 35, alineatul (7), precum și din articolul 5, alineatul (2) (responsabilitatea), coroborat cu articolul 24, alineatul (1) și articolul 36, alineatul (3), litera (e) (care impune autorității de supraveghere să furnizeze „evaluarea impactului asupra protecției datelor prevăzută la articolul 35”). De asemenea, revizuirea cerută de articolul 35, alineatul (11), pentru a evalua dacă prelucrarea este efectuată în conformitate cu EIPD, impune menținerea rezultatelor evaluării impactului. În plus, raportarea unei evaluări a impactului asupra confidențialității este în conformitate cu bunele practici globale din acest domeniu, care se bazează în mod evident pe articolul 35 al RGPD.

Se recomandă ca procesul EIPD să fie însoțit de documentație, în sensul unui „document viu”, începând cu analiza valorii pragului, în cazul în care nu este necesară realizarea unei EIPD. Chiar dacă analiza arată că EIPD nu este necesară și procesul este anulat, operatorul este în continuare responsabil pentru ceea ce s-a realizat și trebuie să furnizeze dovezi în acest sens. Documentația scrisă poate fi transmisă supraveghetorului în orice proces ulterior și va urmări considerațiile și evaluările interne.

În ceea ce privește conținutul, raportul EIPD stabilește, în esență, procedura (inclusiv prezentarea faptelor în sensul unei descrieri sistematice a întregului subiect al testării – „obiectivul evaluării”) și rezultatele procesului EIPD. Ca și în cazul procesului EIPD în sine, RGPD nu prevede nicio regulă specifică pentru elaborarea raportului. Cu toate acestea, criteriile enumerate de Grupul de lucru ”Articolul 29” în Anexa 2 a WP248, care se bazează pe articolul 35, alineatul (7) al RGPD, stabilesc un conținut minim. ISO / IEC 29134 recomandă următorul conținut al raportului privind evaluarea impactului asupra confidențialității, punând accent pe evaluarea riscurilor:

1. Cerințele de confidențialitate relevante.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

2. Descrierea domeniului de aplicare.
3. Descrierea criteriilor de risc utilizate.
4. Participanții la implementare.
5. Părțile interesate consultate.

Acest lucru este susținut și de considerentul 90, care prevede, printer altele, următoarele: *„[r]espectiva evaluare a impactului ar trebui să includă, în special, măsurile, garanțiile și mecanismele avute în vedere pentru atenuarea riscului respectiv, pentru asigurarea protecției datelor cu caracter personal și pentru demonstrarea conformității cu prezentul regulament.”*

În detaliatul studiu PIAF, un raport privind evaluarea impactului asupra confidențialității are următorul conținut minim:[5]

1. Introducere și informații de fond, inclusiv cine realizează evaluarea, detalii de contact și unde pot fi obținute informații suplimentare sau alte surse utile ori recomandări.
2. O descriere a proiectului, a fluxurilor de informații și a impactului asupra confidențialității.
3. Rezultatele consultării părților interesate.
4. Descrierea etapelor de evaluare a riscurilor și de atenuare a acestora, inclusiv alternativele luate în considerare.
5. Analiza conformității juridice.
6. Recomandări.
7. Anexe, dacă este cazul.

În cazul în care raportul sau ultima variantă de lucru sunt disponibile, se ridică întrebarea cu privire la ce ar trebui să se întâmple cu persoana responsabilă (intern), dacă și de către cine ar trebui să fie aprobate – o chestiune practică relevantă, care nu este menționată în RGPD. ICO stipulează în mod explicit în Codul său de practică: „ se obține semnătura adecvată în cadrul organizației”. Deoarece persoana responsabilă trebuie să ducă la bun sfârșit EIPD, rezultă că reprezentanții autorizați ai acesteia sunt implicați în EIPD și au, de asemenea, răspunderea finală. Conducerea va avea, de obicei, autoritate decizională definitivă asupra subiectului și naturii proiectului EIPD. Ca varinată minimă, managerul de proiect sau responsabilul cu protecția datelor trebuie să

5 *De Hert/Kloza/Wright* (Hrsg), PIAF, Recommendations for a privacy impact assessment framework for the European Union, Deliverable D3 (2012) 31, http://piafproject.eu/ref/PIAF_D3_final.pdf.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

raporteze la „cel mai înalt nivel al conducerii”, așa cum este prevăzut la articolul 38, alineatul (3) din RGPD.

RGPD nu obligă la publicarea EIPD, însă WP29 recomandă ca aceasta să fie făcută (cel puțin parțial), pentru a spori încrederea în prelucrarea datelor și pentru a promova transparența. În special, publicarea este încurajată în cazurile în care o parte din public va fi afectată de prelucrare (planificată).

5. Concluzii și recomandări

În special, agențiile de reglementare bine finanțate și-au dezvoltat pe parcursul anilor propriile abordări privind evaluarea impactului asupra confidențialității. În ziua de azi, este de așteptat ca acele autorități pentru protecția datelor care și-au dezvoltat deja propriile modele să prefere să lucreze cu ele sau să le transfere mai departe, nu în ultimul rând deoarece cunoștințele autorităților de supraveghere respective în ceea ce privește propriile recomandări vor fi cele mai pronunțate. Conținuturile modelelor autorităților de supraveghere naționale (din statele membre ale UE) existente în prezent au, deseori, prioritate față de RGPD și nu sunt (încă) adaptate în mod consecvent cerințelor sau terminologiei RGPD.

Cu toate acestea, ICO a adăugat Codul său de practică cu privire la evaluarea impactului asupra confidențialității (2014) în raportul "Big data, artificial intelligence, machine learning and data protection"[6], care este adaptat cerințelor și terminologiei RGPD, astfel încât e de așteptat ca și alte autorități de protecție a datelor să procedeze în mod similar. De asemenea, rămâne de văzut în ce măsură Comitetul european pentru protecția datelor (articolul 68) va furniza linii directoare, recomandări și/sau bune practici pentru EIPD în conformitate cu articolul 70, alineatul (1), liera (e).

Recomandări:

- Documentarea tuturor deciziilor, în special de ce nu a fost efectuată EIPD (dacă este cazul);
- Dacă aveți îndoieli, efectuați EIPD;
- Implicarea părților interesate interne și externe;
- Utilizarea modelelor, a bunelor practici și, dacă este cazul, a EIPD similare deja existente;
- Publicarea EIPD:

[6] ICO, Big data, artificial intelligence, machine learning and data protection (2017), 99, https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

- În special de către autoritățile publice;
- Crește gradul de conștientizare a confidențialității și sporește încrederea.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

6. Bibliografie

6.1. Cărți și articole

- ***Kastelitz, M., Hötzendorfer, W., Riedl, R***., Ausgewählte Fragen der Durchführung einer Datenschutz-Folgenabschätzung gemäß Art 35 DSGVO, Jahrbuch Datenschutzrecht 2017, 113ff.
- ***De Hert, Paul/Kloza, Dariusz/Wright, David,*** Recommendations for a privacy impact assessment framework for the European Union http://www.piafproject.eu/ref/PIAF_D3_final.pdf
- ***Wright, David/De Hert, Paul* (Ed.),** Privacy Impact Assessment, Springer Science & Business Media, Dordrecht, Heidelberg, London, New York 2012
- ***De Hert/Kloza/Wright*** (Ed.), **PIAF**, Recommendations for a privacy impact assessment framework for the European Union, Deliverable D3 (2012), http://piafproject.eu/ref/PIAF_D3_final.pdf; http://piafproject.eu/Deliverables.html.
- ***Martini in Paal/Pauly*** (Ed.), Datenschutz-Grundverordnung (2016) Art 35 Rz 60; dagegen (mangels rechtlicher Verbundenheit) Laue/Nink/Kremer, Das neue Datenschutzrecht in der betrieblichen Praxis (2016) 245 Rz 99.

6.2. Documente referitoare la Grupul de lucru ”Articolul 29”

- Artikel-29-Working Party, WP 248, April 4, 2017: Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679 http://ec.europa.eu/newsroom/document.cfm?doc_id=44137
- WP 248, as last Revised and adopted on 4 October 2017 (rev.01): Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679 https://www.dsb.gv.at/documents/22758/112500/Guidelines_on_Data_Protection_Impact_Assessment_(DPIA).pdf/ed5daa8c-d388-43a6-9842-629b8175a99c

6.3. Link-uri Web

- Brussels Laboratory for Data Protection and Privacy Impact Assessments http://www.vub.ac.be/LSTS/dpialab/

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

- ICO, Big data, artificial intelligence, machine learning and data protection (2017), 99, https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

ProLegis

Transparența

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

ProLegis

Cuprins

1. CADRU LEGAL 4
   1.1. *Versiunea consolidată a Tratatelor Uniunii Europene* 4
   1.2. *Carta drepturilor fundamentale a Uniunii Europene* 4
   1.3. *RGPD* 4
2. SEMNIFICAȚIA TRANSPARENȚEI CONFORM RGPD 5
   2.1. Elementele transparenței (articolul 12 din RGPD) 6
      2.1.1. „Concisă, transparentă, inteligibilă și ușor accesibilă” 6
      2.1.2. „Limbaj clar și simplu” 6
      2.1.3. Modul de furnizare a informațiilor (articolul 12, alineatul (1) și alineatul (5) – „fără taxe” 7
   2.2. Informațiile care se furnizează persoanelor vizate (articolul 13 și articolul 14) ... 7
      2.2.1. Ce informații ar trebui furnizate? 7
      2.2.3 Cum ar trebui furnizate informațiile? 8
      2.2.4. Când ar trebui furnizate informațiile? 9
      2.2.5. Când ar trebui operatorii să transmită notificări în cazul modificărilor aduse transparenței informațiilor? 9
   2.3. Modalitățile 10
      2.3.1. Notificările / declarațiile de confidențialitate 10
      2.3.2. Notificările “Push” & “pull” 10
      2.3.3. Alte tipuri de „măsuri adecvate” 10
      2.3.4. Vizualizarea 11
   2.4. Exercitarea drepturilor persoanei vizate 11
3. CONCLUZIE ȘI RECOMANDĂRI 12
4. BIBLIOGRAFIE 13
   Cărți 13

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

Documente referitoare la Grupul de lucru ”Articolul 29” 13
Link-uri web..... 13
5. NOTE..... 13

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

1. CADRU LEGAL

1.1. Versiunea consolidată a Tratatelor Uniunii Europene

Articolul 1 al Tratatului privind Uniunea Europeană (TUE) -> deciziile se iau „cu respectarea deplină a principiului transparenței și cât mai aproape cu putință de cetățeni”;

Articolul 11, alineatul (2) al TUE -> „Instituțiile Uniunii mențin un dialog deschis, transparent și constant cu asociațiile reprezentative și cu societatea civilă”;

Articolul 15 al Tratatului privind funcționarea Uniunii Europene (TFUE) -> cetățenii Uniunii au dreptul să acceseze documentele instituțiilor, organismelor, oficiilor și agențiilor Uniunii, iar acestea au la rândul lor obligația să asigure transparența procedurilor.

1.2. Carta drepturilor fundamentale a Uniunii Europene

Transparența este esențială pentru prelucrarea corectă. Din acest motiv, este cuprinsă în articolul 8 al Cartei drepturilor fundamentale a UE.

Articolul 8

Protecția datelor cu caracter personal

1. Orice persoană are dreptul la protecția datelor cu caracter personal care o privesc.

2. Asemenea date trebuie tratate ***în mod corect****, în scopurile precizate și pe baza consimțământului persoanei interesate sau în temeiul unui alt motiv legitim prevăzut de lege. Orice persoană are dreptul de acces la datele colectate care o privesc, precum și dreptul de a obține rectificarea acestora.*

3. Respectarea acestor norme se supune controlului unei autorități independente.

1.3. RGPD

Considerentul 39

Ar trebui să fie transparent pentru persoanele fizice că sunt colectate, utilizate, consultate sau prelucrate în alt mod datele cu caracter personal care le privesc și în ce măsură datele cu caracter personal sunt sau vor fi prelucrate. Principiul transparenței prevede că orice informații și comunicări referitoare la prelucrarea respectivelor date cu caracter personal sunt ușor accesibile și ușor de înțeles și că se utilizează un limbaj simplu și clar. Acest principiu se referă în special la informarea persoanelor vizate privind identitatea operatorului și scopurile prelucrării, precum și la

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

oferirea de informații suplimentare, pentru a asigura o prelucrare echitabilă și transparentă în ceea ce privește persoanele fizice vizate și dreptul acestora de a li se confirma și comunica datele cu caracter personal care le privesc care sunt prelucrate…

Considerentul 58

Principiul transparenței prevede că orice informații care se adresează publicului sau persoanei vizate să fie concise, ușor accesibile și ușor de înțeles și să se utilizeze un limbaj simplu și clar, precum și vizualizare acolo unde este cazul. Aceste informații ar putea fi furnizate în format electronic, de exemplu atunci când sunt adresate publicului, prin intermediul unui site. Acest lucru este important în special în situații în care datorită multitudinii actorilor și a complexității, din punct de vedere tehnologic, a practicii, este dificil ca persoana vizată să știe și să înțeleagă dacă datele cu caracter personal care o privesc sunt colectate, de către cine și în ce scop, cum este cazul publicității online. Întrucât copiiii necesită o protecție specifică, orice informații și orice comunicare, în cazul în care prelucrarea vizează un copil, ar trebui să fie exprimate într-un limbaj simplu și clar, astfel încât copilul să îl poată înțelege cu ușurință.

Articolul 5

Principii legate de prelucrarea datelor cu caracter personal

1. Datele cu caracter personal sunt:

(a) prelucrate în mod legal, echitabil și transparent față de persoana vizată („legalitate, echitate și transparență”);

2. SEMNIFICAȚIA TRANSPARENȚEI CONFORM RGPD

Principiul transparenței se află în strânsă legătură cu principiile corectitudinii și responsabilității. Articolul 5 al RGPD (Principii legate de prelucrarea datelor cu caracter personal) obligă operatorii să demonstreze că datele sunt prelucrate în mod transparent. Potrivit Grupului de lucru ”Articolul 29”[i], transparența le permite persoanelor vizate să îi facă responsabili pe operatori și pe persoanele împuternicite de operator și, totodată, să dețină controlul asupra propriilor date cu caracter personal[ii]. Acest lucru se realizează prin introducerea unor cerințe practice specifice care trebuie respectate în toate etapele prelucrării: înainte sau la începutul prelucrării datelor, în momentul colectării datelor și pe întreaga perioadă a prelucrării.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

2.1. Elementele transparenței (articolul 12 din RGPD)

2.1.1. „Concisă, transparentă, inteligibilă și ușor accesibilă”

Primele două elemente ale acestei cerințe se referă la faptul că operatorii de date au obligația să prezinte informațiile / să comunice în mod eficient și într-o manieră succintă pentru a evita suprasolicitarea persoanelor vizate (altfel spus, pentru a nu copleși persoanele vizate cu informații). Acest lucru poate fi realizat cu ajutorul notificărilor stratificate, atunci când persoanelor vizate li se prezintă pas cu pas drepturile (de exemplu, prin furnizarea informațiilor cheie într-o notificare scurtă, iar restul în momentul colectării datelor). Aceste informații trebuie să fie separate de alte informații care nu privesc confidențialitatea, cum ar fi prevederile contractuale.

Cerința ca informația să fie „inteligibilă” înseamnă că ar trebui să fie înțeleasă de o persoană de nivel mediu din publicul țintă, în cazul de față, de cetățeanul de nivel mediu al comunității locale. Persoanele vizate ar trebui să poată determina în avans care sunt domeniul de aplicare și consecințele prelucrării. Grupul de lucru ”Articolul 29” (WP29) le recomandă operatorilor să precizeze într-un limbaj lipsit de ambiguitate care vor fi cele mai importante consecințe ale prelucrării, mai ales dacă astfel de consecințe pot avea un impact asupra drepturilor fundamentale ale persoanelor vizate[iii].

Elementul „ușor accesibilă” vizează accesarea fără efort a informației de către persoana vizată. În acest sens, aceasta nu ar trebui să caute informațiile, ci, dimpotrivă, ar trebui să le primească într-o manieră evidentă.

2.1.2. „Limbaj clar și simplu”

Cerința unui limbaj clar și simplu prevede că informațiile trebuie să fie furnizate într-un mod cât mai simplu posibil, evitând enunțurile și structurile lingvistice complexe. Informațiile nu trebuie să fie formulate în termeni abstracți sau ambivalenți sau să lase loc interpretărilor diferite[iv]. Temeiul juridic și scopurile prelucrării datelor cu caracter personal trebuie să fie clare. Orice formulare neclară a scopurilor prelucrării trebuie evitată (de exemplu, „pentru dezvoltarea unor viitoare servicii” sau ”în scopuri de cercetare”). Informațiile furnizate persoanei vizate nu ar trebui să conțină un limbaj sau o terminologie prea legalistă, tehnică sau de specialitate[v].

Autoritățile locale ar trebui, de asemenea, să se asigure că vocabularul, tonul și stilul limbajului utilizat în raport cu copiii este adecvat și rezonează cu aceștia, astfel încât ei să poată recunoaște că mesajul / informațiile le sunt adresate[vi].

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

2.1.3. Modul de furnizare a informațiilor (articolul 12, alineatul (1) și alineatul (5) – „fără taxe”

Operatorii de date nu pot percepe taxe persoanelor vizate pentru furnizarea informațiilor în temeiul articolelor 13 și 14 (informații care se furnizează persoanelor vizate) sau pentru comunicări și acțiuni întreprinse în temeiul articolelor 15-22 (drepturile persoanelor vizate) și al articolului 34 (informarea persoanei vizate cu privire la încălcarea securității datelor cu caracter personal). Există o excepție de la această regulă: atunci când solicitările unei persoane vizate sunt în mod vădit nefondate sau excesive, în special din pricina caracterului repetitiv. În acest caz, operatorul de date poate percepe o taxă rezonabilă, având în vedere costurile administrative de furnizare a informațiilor, de comunicare sau de luare a măsurii solicitate. Este important ca operatorii de date să știe că intră în sarcina lor să demonstreze caracterul vădit nefondat sau excesiv al solicitării. Prin urmare, potrivit RGPD, nu este recomandabil ca autoritățile locale să perceapă taxe cetățenilor pentru furnizarea de informații.

2.2. Informațiile care se furnizează persoanelor vizate (articolul 13 și articolul 14)

2.2.1. Ce informații ar trebui furnizate?

Articolele 13 și 14 din GDPR stipulează ce informații trebuie furnizate persoanei vizate. Regulamentul face distincție între cazurile în care informațiile sunt colectate de la persoana vizată (articolul 13) și cele în care informațiile nu au fost obținute de la aceasta (articolul 14). Autoritățile locale ar trebui să furnizeze:

1) informații referitoare la identitate sa, inclusiv datele de contact;
2) datele de contact ale responsabilului cu protecția datelor;
3) scopurile prelucrării și fundamentarea juridică a acestora – în special pentru autoritățile locale, fundamentarea se regăsește la articolul 6, alineatul (1), litera (e), exercitarea unei autorități oficiale cu care este învestit operatorul și dispozițiile respective din dreptul intern;
4) tipul de date prelucrate, atunci când nu au fost obținute de la persoana vizată;
5) identitatea posibililor destinatari ai datelor – aceasta nu include numai terți, ci și persoane împuternicite de operatori și operatori asociați. Operatorul de date ar trebui să fie cât mai precis în definirea diferitelor categorii de destinatari ai datelor.

2.2.2. Ce informații suplimentare ar trebui furnizate?

În primul rând, pentru a asigura o prelucrare corectă și transparentă, operatorul trebuie să îi furnizeze persoanei vizate:

1) informații referitoare la perioada de stocare a datelor cu caracter personal sau

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

criteriile folosite pentru determinarea perioadei respective;
2) informații cu privire la dreptul persoanei vizate de a solicita accesul la datele cu caracter personal sau rectificarea ori ștergerea acestora, limitarea prelucrării, informații referitoare la dreptul persoanei vizate de a se opune prelucrării, precum și informații privind dreptul la portabilitatea datelor;
3) în cazul în care prelucrarea se bazează pe consimțământ, informații cu privire la dreptul de retragere a acestuia în orice moment;
4) informații privind dreptul de a depune o plângere la o autoritate de supraveghere;
5) informații despre procesele decizionale automate, inclusiv crearea de profiluri, informații relevante cu privire la logica implicată, precum și la semnificația și consecințele preconizate ale unei astfel de prelucrări.

Informațiile despre crearea de profiluri nu numai că ar trebui să le fie ușor accesibile persoanelor vizate, ci să le fie și aduse la cunoștință. Operatorul ar trebui să poată oferi explicații simple pentru logica sau criteriile utilizate în luarea deciziilor automate, fără a intra în detalii referitoare la algoritmii de prelucrare.

În cazul în care datele nu au fost obținute de la persoana vizată, operatorul trebuie să furnizeze sursa. Dacă datele sunt furnizate de către persoana vizată, atunci operatorul are obligația de a o informa pe aceasta, în măsura în care furnizarea de date cu caracter personal este o cerință legală.

În al doilea rând, operatorii trebuie să informeze persoanele vizate dacă intenționează să prelucreze datele în oricare alt scop decât cel pentru care au fost colectate. Persoanelor vizate trebuie să li se furnizeze informații cu privire la acest scop diferit și la orice alte aspecte relevante, exact la fel cum s-a procedat în legătură cu informațiile furnizate în scopul inițial (perioada de prelucrare, temeiul juridic aplicat etc.). Atunci când se obțin date, este utilă informarea persoanelor vizate cu privire la eventuale prelucrări ulterioare, în cazul în care e probabil să se întâmple acest lucru, dată fiind activitatea operatorului.

2.2.3 Cum ar trebui furnizate informațiile?

Modul implicit de furnizare a informațiilor și de comunicare cu persoanele vizate îl reprezintă formatul scris. Totuși, RGPD permite furnizarea informațiilor și prin alte mijloace, inclusiv cele electronice. Conform WP29, esențial este ca metodele alese să fie adecvate cirmustanțelor[vii]. Informațiile pot fi furnizate pe cale orală persoanelor vizate, la cerere, în cazul în care informațiile privind identitatea lor sunt dovedite prin alte mijloace, și anume non-orale[viii]. Există o excepție de la regulă în ceea ce privește informațiile pe care operatorii de date ar trebui să le furnizeze conform articolelor 13 și 14 – aceste informații pot fi dezvăluite subiectului fără verificarea identității. Furnizarea pe cale orală a informațiilor nu înseamnă neapărat informații orale furnizate după modelul persoană-către-persoană, ci și informații orale automatizate. Potrivit WP29, operatorul de date ar

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

trebui să permită persoanei vizate să re-asculte mesajele înregistrate în prealabil, în special atunci când este vorba de persoane care întâmpină dificultăți de accesare sau înțelegere a formatului scris. De asemenea, în cazul furnizării pe cale orală a informațiilor, operatorii au în continuare obligația de a demonstra că au respectat cerințele RGPD. Pentru a realiza acest lucru, ei trebuie să se asigure că au o dovadă cu privire la 1) cererea de informații prin mijloace orale, 2) metoda prin care a fost verificată identitatea persoanei vizate și 3) faptul că informațiile au fost furnizate persoanei vizate[ix].

2.2.4. Când ar trebui furnizate informațiile?

Informațiile privind prelucrarea datelor cu caracter personal ar trebui să fie furnizate persoanei vizate în momentul colectării (articolul 13, alineatul (1)). În cazul în care datele nu sunt obținute direct de la persoana vizată, ci din altă sursă, informațiile trebuie să fie furnizate persoanei vizate într-o perioadă rezonabilă, dar care să nu depășească mai mult de o lună de la data obținerii, în funcție de circumstanțe. Există două situații: în primul rând, atunci când datele sunt utilizate pentru comunicarea cu subiectul, informațiile trebuie furnizate cel târziu în momentul primei comunicări către persoana vizată; în al doilea rând, dacă este de așteptat ca datele să fie dezvăluite altui destinatar, cel târziu la prima dezvăluire față de acesta.

Perioada poate fi extinsă la maximum trei luni, în funcție de complexitatea și numărul solicitărilor (de exemplu, dacă cererea implică accesarea mai multor baze de date). Operatorul trebuie să informeze persoana vizată cu privire la o astfel de prelungire în termen de o lună de la primirea cererii, împreună cu motivele întârzierii și cu informațiile referitoare la dreptul subiectului de a depune o plângere.

2.2.5. Când ar trebui operatorii să transmită notificări în cazul modificărilor aduse transparenței informațiilor?

În situațiile în care schimbarea informațiilor poate avea un impact grav asupra persoanei vizate, controlorii de date ar trebui să furnizeze informații cu mult timp înainte de intrarea efectivă a modificării[x]. Acest lucru ar trebui să fie făcut într-o manieră explicită și eficace. Cetățenii ar trebui să aibă suficient timp pentru a lua în considerare natura și impactul modificărilor și să își exercite drepturile garantate în cadrul RGPD cu privire la modificări, de exemplu să se opună prelucrării. WP29 recomandă să li se reamintească periodic persoanelor vizate de domeniul de aplicare al prelucrării datelor[xi].

Atunci când prelucrarea datelor urmează să fie făcută în alt scop decât cel pentru care a fost obținută, persoanele vizate trebuie să fie informate înainte de începerea noii prelucrări.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

2.3. Modalitățile

Modalitățile reprezintă formatele pe care operatorii de date le au la dispoziție pentru a-și îndeplini obligația furnizării de informații persoanelor vizate în conformitate cu RGPD.

2.3.1. Notificările / declarațiile de confidențialitate

În ceea ce privește platformele online, utilizarea unei abordări a declarațiilor / notificărilor stratificate privind confidențialitatea, care să lege diferitele categorii de informații care trebuie furnizate persoanei vizate, în loc să utilizeze o singură notificare[xii]. Această abordare le permite utilizatorilor să navigheze direct la secțiunea din notificare pe care doresc să o citească. Atunci când fac apel la o astfel de notificare stratificată, operatorii trebuie să își propună să ofere o imagine de ansamblu clară și ușor de înțeles, astfel încât persoanele vizate să știe unde pot găsi fiecare informație.

2.3.2. Notificările “Push” & “pull”

WP29 introduce folosirea notificărilor “push” și “pull”. Principala deosebire este că, în cazul celor din urmă, utilizatorii unui site sunt de așteptat să solicite informații despre prelucrarea datelor lor, pe când în cazul primelor, notificarea este „împinsă” pe ecranul lor fără ca aceștia să întreprindă vreo acțiune. WP29 definesc și exemplifică notificările “push” prin notificări de informare transparente de tipul „tocmai la timp”, iar notificările “pull” prin panouri de bord transparente și tutoriale de tipul „aflați mai multe”[xiii]:

- *Notificarea tocmai la timp* este utilizată pentru a furniza informații cu caracter confidențial specifice, atunci când este important pentru persoana vizată să le citească. Acest format se dovedește util în situația în care un site web al unei autorități locale prevede efectuarea unui anumit serviciu online după completarea unui formular. Înainte de trimiterea formularului, cetățeanului îi poate apărea o notificare *tocmai la timp*.
- *Panourile de bord transparente* reprezintă un singur punct de la care persoanele vizate pot vizualiza informații cu caracter confidențial și își pot gestiona preferințele de confidențialitate, permițând sau împiedicând utilizarea datelor în anumite moduri.

2.3.3. Alte tipuri de „măsuri adecvate”

În afara mediului digital, alte măsuri adecvate în conformitate cu WP29 pot fi:

- Pentru mediul tipărit / hârtie: explicații scrise, pliante;
- Pentru mediul telefonic: explicații orale oferite de o persoană reală, informații automatizate sau pre-înregistrate, cu opțiuni de a auzi informații mai detaliate;
- Coduri QR, alerte vocale, informații scrise pe dispozitive inteligente, mesaje trimise prin SMS sau e-mail și altele;

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

- Pentru mediul persoană-către-persoană: explicații orale sau scrise oferite în format hard sau soft[xiv].

2.3.4. Vizualizarea

RGPD introduce instrumente de vizualizare, referindu-se în special la pictograme, mecanisme de certificare, sigilii și mărci pentru protecția datelor. Pictogramele au rolul de a transmite informațiile persoanelor vizate într-un mod accesibil, utilizând simboluri / imagini standardizate, recunoscute în întreaga UE. Dezvoltarea unui „cod al pictogramelor" nu a început încă. RGPD prevede, de asemenea, utilizarea mecanismelor de certificare, a sigiliilor și mărcilor pentru protecția datelor în scopul demonstrării conformității cu regulamentul. Mecanismele de certificare sunt stabilite de statele membre, autoritățile de supraveghere, organismul european de protecție a datelor sau de Comisia Europeană și sunt destinate să demonestreze că operatorul respectă RGPD prin aplicarea unor măsuri tehnice și organizatorice care conduc la atingerea standardelor de protecție a datelor. Aceste formate pot fi aplicate și în instituții care nu sunt autorități publice, cum ar fi o companie municipală autonomă.

2.4. Exercitarea drepturilor persoanei vizate

Persoanele vizate au dreptul să primească informații de la operatori cu privire la datele lor cu caracter personal. Informațiile care trebuie furnizate conform RGPD sunt enumerate explicit în articolul 13 și articolul 14, iar persoanele vizate nu trebuie să depună o cerere sau să ia alte măsuri pentru a le obține, spre deosebire de cazurile în care își exercită celelalte drepturi conexe (dretul de acces, rectificare, ștergere etc.).

2.4.1. Excepții de la obligația de a furniza informații

Dreptul la informație nu este absolut, ci este limitat la anumite situații.
În anumite cazuri, autoritățile locale sunt scutite de obligația de a furniza informațiile menționate mai sus, prevăzute la art. 13 și 14. Atunci când datele sunt obținute de la persoana vizată, nu mai trebuie să îi fie furnizate informații dacă le deține deja (articolul 13, alineatul (4)). Atunci când datele nu sunt obținute la de persoana vizată, există mai multe situații (articolul 14, alineatul (5)):

- persoana vizată deține deja informațiile;
- furnizarea acestor informații se dovedește a fi imposibilă sau ar implica eforturi disproporționate, sau fac imposibilă ori afectează grav realizarea obiectivelor prelucrării; un exemplu al imposibilității de a fruniza informații ar fi atunci când operatorul nu dispune de niciun mijloc pentru contactarea persoanei vizate;
- obținerea sau divulgarea datelor este prevăzută în mod expres de dreptul Uniunii sau de dreptul intern – acesta este scenariul cel mai des întâlnit la nivelul

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

autorităților locale;

- în cazul în care datele cu caracter personal fac obiectul unei obligații statutare de secret profesional reglementate de dreptul Uniunii sau de dreptul intern, inclusiv al unei obligații legale de a păstra secretul; această excepție poate fi aplicată companiilor municipale autonome și entităților similare.

Conform WP29[xv], aceste excepții ar trebui interpretate și aplicate în sens restrâns.

3. CONCLUZIE ȘI RECOMANDĂRI

Principiul transparenței este unul dintre fundamentele RGPD. Acesta garantează în diverse moduri că persoanele fizice dispun de toate informațiile de care au nevoie pentru a fi informate cu privire la datele cu caracter personal care le sunt prelucrate și la drepturile pe care și le pot exercita în virtutea regulamentului. Informațiile trebuie să fie ușor accesibile, ușor de înțeles și exprimate într-un limbaj clar și simplu.

Autorităților locale li se recoamndă să facă o listă cu toate informațiile solicitate de RGPD și să aleagă cele mai bune modalități de a ajunge la cetățenii cărora le prelucrează datele. De exemplu, pot pune la îndemână fișe informative în birourile publice și pot crea și distribui pliante care să cuprindă informațiile prevăzute la articolele 13 și 14. Mijloacele electronice pot fi utile, de exemplu, dacă instituția are un site / o platformă online, însă, în anumite cazuri, se impun și formatele tipărite. O atenție sporită ar trebui acordată situațiilor în care portalurile web ale autorităților locale oferă servicii online. De asemenea, ar trebui să se țină cont de faptul că unele companii municipale autonome (cum ar fi companiile de transport public) execută numeroase tipuri de prelucrări și gestionează baze de date enorme, prin urmare acestea ar trebui să depună eforturi suplimentare pentru aplicarea corectă a informațiilor prevăzute la articolele 13 și 14.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

4. BIBLIOGRAFIE

Cărți

- **Voigt, P., von dem Bussche, A.**, The EU General Data Protection Regulation (GDPR) – A Practical Guide, Springer International Publishing (2017);
- Bird & Bird Guide to General Data Protection Regulation (2016);
- EU General Data Protection Regulation (GDPR). An Implementation and Compliance Guide, IT Governance Publishing, Cambridgeshire (2016);

Documente referitoare la Grupul de lucru ”Articolul 29”

- Article 29 Working Party, Guidelines on Data Protection Officers (‘DPOs’), WP 243 rev.01;
- Article 29 Working Party, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, WP 217;

Link-uri web

- http://europa.eu/rapid/press-release_IP-18-386_en.htm
- https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en

5. NOTE

[i] Grupul de lucru ”Articolul 29” (WP29) a fost stabilit în temeiul Art. 29 al Directivei 95/46/CE, care este este înlocuită de RGPD. Scopul grupului de lucru este să formuleze opinii și recomandări și să ofere consiliere cu privire la protecția datelor cu caracter personal.
[ii] Article 29 Data Protection Working Party, Guidelines on transparency under Regulation 2016/679, p. 23
[iii] Ibid, p. 8
[iv] Ibid, p. 9
[v] Ibid
[vi] Ibid
[vii] Ibid, p. 21
[viii] Ibid, p. 11
[ix] Ibid, p. 12
[x] Ibid, p. 15
[xi] Ibid, p. 16
[xii] Ibid, p. 17
[xiii] Ibid, p. 17-18
[xiv] Ibid, p. 18-19
[xv] Ibid, p. 25

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

ProLegis

Divulgarea Informațiilor sau Dreptul de Acces al Persoanei Vizate

Articolul 15 RGPD

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

ProLegis

Cuprins

1. Cadru legal 3

1.1. Regulamentul general privind protecția datelor (RGPD) 3

2. Elemente de bază 5

3. Detalii privind divulgarea informațiilor către persoana vizată 5

3.1. Substanța divulgării 5

3.2. Cât timp are operatorul la dispoziție pentru a oferi un răspuns (termenul limită)? 7

3.3. Ce formă poate lua solicitarea și cum ar trebui să i se răspundă? 7

3.4. Trebuie făcută dovada identității solicitantului? 8

3.5. Costuri? Pot fi rambursate informațiile? 9

3.6. Are solicitantul obligația de a participa la divulgarea informațiilor? 9

3.7. Trebuie să fie luate în considerare drepturile terților atunci când sunt furnizate informații? 9

4. Listă de verificare pentru divulgarea informațiilor la cerere 10

4.1. Emiterea informațiilor 11

5. Bibliografie 12

5.1. Cărți și articole 12

5.2. Alte documente și cazuri 12

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

1. Cadru legal

1.1. Regulamentul general privind protecția datelor (RGPD)

Articolul 15

Dreptul de acces al persoanei vizate

(1) Persoana vizată are dreptul de a obține din partea operatorului o confirmare că se prelucrează sau nu date cu caracter personal care o privesc și, în caz afirmativ, acces la datele respective și la următoarele informații:

(a) scopurile prelucrării;

(b) categoriile de date cu caracter personal vizate;

(c) destinatarii sau categoriile de destinatari cărora datele cu caracter personal le-au fost sau urmează să le fie divulgate, în special destinatari din țări terțe sau organizații internaționale;

(d) acolo unde este posibil, perioada pentru care se preconizează că vor fi stocate datele cu caracter personal sau, dacă acest lucru nu este posibil, criteriile utilizate pentru a stabili această perioadă;

(e) existența dreptului de a solicita operatorului rectificarea sau ștergerea datelor cu caracter personal ori restricționarea prelucrării datelor cu caracter personal referitoare la persoana vizată sau a dreptului de a se opune prelucrării;

(f) dreptul de a depune o plângere în fața unei autorități de supraveghere;

(g) în cazul în care datele cu caracter personal nu sunt colectate de la persoana vizată, orice informații disponibile privind sursa acestora;

(h) existența unui proces decizional automatizat incluzând crearea de profiluri, menționat la articolul 22 alineatele (1) și (4), precum și, cel puțin în cazurile respective, informații pertinente privind logica utilizată și privind importanța și consecințele preconizate ale unei astfel de prelucrări pentru persoana vizată.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

(2) În cazul în care datele cu caracter personal sunt transferate către o țară terță sau o organizație internațională, persoana vizată are dreptul să fie informată cu privire la garanțiile adecvate în temeiul articolului 46 referitoare la transfer.

(3) Operatorul furnizează o copie a datelor cu caracter personal care fac obiectul prelucrării. Pentru orice alte copii solicitate de persoana vizată, operatorul poate percepe o taxă rezonabilă, bazată pe costurile administrative. În cazul în care persoana vizată introduce cererea în format electronic și cu excepția cazului în care persoana vizată solicită un alt format, informațiile sunt furnizate într-un format electronic utilizat în mod curent.

4) Dreptul de a obține o copie menționată la alineatul (3) nu aduce atingere drepturilor și libertăților altora.

Considerentele 63 și 64:

(63) O persoană vizată ar trebui să aibă drept de acces la datele cu caracter personal colectate care o privesc și ar trebui să își exercite acest drept cu ușurință și la intervale de timp rezonabile, pentru a fi informată cu privire la prelucrare și pentru a verifica legalitatea acesteia. Acest lucru include dreptul persoanelor vizate de a avea acces la datele lor privind sănătatea, de exemplu datele din registrele lor medicale conținând informații precum diagnostice, rezultate ale examinărilor, evaluări ale medicilor curanți și orice tratament sau intervenție efectuată. Orice persoană vizată ar trebui, prin urmare, să aibă dreptul de a cunoaște și de a i se comunica în special scopurile în care sunt prelucrate datele, dacă este posibil perioada pentru care se prelucrează datele cu caracter personal, destinatarii datelor cu caracter personal, logica de prelucrare automată a datelor cu caracter personal și, cel puțin în cazul în care se bazează pe crearea de profiluri, consecințele unei astfel de prelucrări. Dacă acest lucru este posibil, operatorul de date ar trebui să poată furniza acces de la distanță la un sistem sigur, care să ofere persoanei vizate acces direct la datele sale cu caracter personal. Acest drept nu ar trebui să aducă atingere drepturilor sau libertăților altora, inclusiv secretului comercial sau proprietății intelectuale și, în special, drepturilor de autor care asigură protecția programelor software. Cu toate acestea, considerațiile de mai sus nu ar trebui să aibă drept rezultat refuzul de a furniza toate informațiile persoanei vizate. Atunci când operatorul prelucrează un volum mare de informații privind persoana vizată, operatorul ar trebui să poată solicita ca, înainte de a îi fi furnizate informațiile, persoana vizată să precizeze informațiile sau activitățile de prelucrare la care se referă cererea sa.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

(64) Operatorul ar trebui să ia toate măsurile rezonabile pentru a verifica identitatea unei persoane vizate care solicită acces la date, în special în contextul serviciilor online și al identificatorilor online. Un operator nu ar trebui să rețină datele cu caracter personal în scopul exclusiv de a fi în măsură să reacționeze la cereri potențiale.

2. Elemente de bază

RGPD prevede la articolul 15 dreptul de a divulga toate informațiile disponibile despre persoana vizată la cererea acesteia (de exemplu, clientului, angajatului, solicitantului de locuri de muncă, pacienților, denumite în continuare „persoana vizată") de către operatorul de prelucrare a datelor cu caracter personal (de exemplu, compania, angajatorul, conducerea spitalului). Acesta este denumit „dreptul de acces al persoanei vizate" (la datele sale). Scopul acestui drept este ca persoana vizată să poată obține informații cu privire la conținutul și detaliile datelor prelucrate despre ea sau el, pentru a permite eventual exercitarea altor drepturi (de exemplu, corectarea sau ștergerea, în conformitate cu articolul 16 al RGPD) sau pentru a asigura legalitatea prelucrării.

Acest drept reprezintă o instituție centrală a legii privind protecția datelor, deoarece este considerat adesea ca baza exercitării altor drepturi de către persoana vizată. Deși în cadrul RGPD autoritățile de protecție a datelor au puterea de a audita un operator fără a exista vreo plângere, în practică, dacă se apelează la acestea, divulgările ajung, de obicei (din cauza resurselor limitate ale autorităților), să fie incomplete sau întârziate. Prin urmare, operatorii ar trebui să fie bine pregătiți pentru un asemenea proces.

Cea mai bună pregătire constă într-o bună structurare și în înregistrări cât mai detaliate ale activităților de prelucrare. Cu cât documentația este mai bine întocmită, cu atât pot fi găsite mai ușor, în timp util, datele specifice unui anumit subiect în cadrul aplicațiilor.

3. Detalii privind divulgarea informațiilor către persoana vizată

3.1. Substanța divulgării

Dreptul de acces îi conferă persoanei vizate următoarele:

i. Dreptul de a-i cere operatorului să confirme dacă datele sale personale sunt prelucrate; dacă e necesar, în cazul în care datele persoanei vizate nu sunt prelucrate, ar trebui să fie oferit un răspuns „negativ" (așa-numitele „informații negative"): „Nu vor fi prelucrate datele dumneavoastră cu caracter personal.";

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

ii. Dreptul de a obține o copie a datelor cu caracter personal care fac obiectul prelucrării (pentru orice copie suplimentară solicitată de persoana vizată, operatorul poate percepe o taxă rezonabilă în funcție de cheltuielile administrative). Dacă persoana vizată depune o cerere în format electronic, atunci informațiile sunt furnizate tot în format electronic, cu excepția cazului în care este prevăzut altfel.

iii. Dreptul de a obține următoarele informații:

Art 15 (1) RGPD	Conținutul informațiilor
lit a	**scopurile prelucrării**
lit b	**categoriile** de date cu caracter personal vizate
lit c	**destinatarii sau categoriile de destinatari** cărora datele cu caracter personal le-au fost sau urmează să le fie divulgate, în special destinatari din țări terțe sau organizații internaționale
lit d	acolo unde este posibil, **perioada pentru care se preconizează că vor fi stocate datele cu caracter personal** sau, dacă acest lucru nu este posibil, criteriile utilizate pentru a stabili această perioadă
lit e	**existența dreptului de a solicita operatorului rectificarea sau ștergerea datelor cu caracter personal ori restricționarea prelucrării datelor cu caracter personal** referitoare la persoana vizată sau a dreptului de a se opune prelucrării
lit f	**dreptul de a depune o plângere** în fața unei autorități de supraveghere
lit g	în cazul în care datele cu caracter personal nu sunt colectate de la persoana vizată, **orice informații disponibile privind sursa acestora**
lit h	existența unui **proces decizional automatizat incluzând crearea de profiluri**, menționat la articolul 22 alineatele (1) și (4), precum și, cel puțin în cazurile respective, informații pertinente privind logica utilizată și privind importanța și consecințele preconizate ale unei astfel de prelucrări pentru persoana vizată
Art 15 (2) RGPD	În cazul în care datele cu caracter personal sunt **transferate către o țară terță sau o organizație**

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

	internațională, persoana vizată are dreptul să fie informată cu privire la garanțiile adecvate în temeiul articolului 46 referitoare la transfer.

Notă: În conformitate cu articolul 23, **dreptul la informație poate fi restricționat de legislația națională.**

3.2. Cât timp are operatorul la dispoziție pentru a oferi un răspuns (termenul limită)?

În principiu, solicitării de informații trebuie să i se răspundă cu promptitudine, însă nu mai târziu de o lună de la primirea cererii (articolul 12, alineatul (3) din RGPD). Această perioadă poate fi prelungită cu încă două luni, dacă este necesar, în funcție de complexitatea și numărul cererilor. Operatorul informează persoana vizată despre prelungirea termenului limită în cel mult o lună de la primirea cererii, împreună cu motivele întârzierii. În cazul în care persoana în cauză depune cererea în format electronic, aceasta trebuie, dacă este posibil, să fie informată tot prin mijloace electronice, cu excepția cazului în care se specifică altfel.

În cazul în care operatorul nu acționează la cererea persoanei vizate, va trebui să o informeze imediat pe aceasta, însă nu mai târziu de o lună de la primirea cererii, invocând motivele corespunzătoare și, de asemenea, aducând la cunoștință despre posibilitatea depunerii unei plângeri în fața autorității de supraveghere sau a acționării în instanță.

3.3. Ce formă poate lua solicitarea și cum ar trebui să i se răspundă?

Nu există nicio constrângere cu privire la formă, solicitarea informațiilor putând fi făcută oral, în scris sau în format digital (de exemplu, prin e-mail). Răspunsul poate lua orice formă adecvată, însă trebuie semnalate următoarele aspecte:

- Dacă solicitarea este în scris, cel mai bine este să i se răspundă în scris. O metodă utilizată în trecut a fost ca reclamantul să depună alături de cerere copia unui act de identitate (oficial), iar persoana responsabilă să transmită răspunsul printr-o scrisoare recomandată (cu excepția agenților de livrare). Cu toate acestea, întrucât actul de identitate conține, de obicei, mai multe date decât ar fi necesar pentru identificarea persoanei vizate, se recomandă ca aceasta să transmită în scris numai informații referitoare la nume, cod numeric personal, seria și numărul actului de identitate.
- La cererea solicitantului, informațiile pot fi furnizate oral, cu condiția ca identitatea persoanei vizate să fi fost stabilită într-o altă formă.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

- În cazul în care persoana vizată transmite cererea în format electronic (de exemplu, prin e-mail), informațiile se furnizează tot în format electronic, dacă nu este prevăzut altfel. Dacă este posibil, operatorul poate, de asemenea, să ofere acces la distanță la un sistem securizat, care oferă persoanei vizate accesul direct la informațiile sale personale.

Atenție! Toate comunicările trebuie transmise într-un limbaj simplu și clar, într-o formă precisă, transparentă, inteligibilă și ușor accesibilă (aceasta se aplică în special informațiilor destinate copiilor). Ca și în trecut, abrevierile conținute în răspuns trebuie să fie explicate de către operator.

3.4. Trebuie făcută dovada identității solicitantului?

Da. Identitatea persoanei care solicită informațiile (persoana în cauză) trebuie să fie clară, deoarece operatorul poate solicita informații suplimentare dacă are „îndoieli rezonabile" cu privire la identitatea persoanei fizice care depune cererea (a se vedea articolul 12, alineatul (6)[1]).

Conform considerentului 64, operatorul trebuie să utilizeze toate mijloacele rezonabile pentru a verifica identitatea persoanei vizate care solicită informații, în special în contextul serviciilor online și în cazul identificatorilor online.

Autentificarea identității ar trebui concepută în așa fel încât să îndeplinească obligația de a asigura securitatea datelor în conformitate cu riscul. În caz contrar, ar putea apărea o încălcare a securității datelor, dacă acestea sunt transmise destinatarului greșit.

O practică obișnuită în Austria, în temeiul precedentei legi privind protecția datelor (DSG 2000), a fost ca solicitantul să depună alături de cerere o copie a actului de identitate, iar operatorul să transmită răspunsul cu poșta, printr-o scrisoare recomandată (cu excepția agenților autorizați). Însă, identitatea poate fi, de asemenea, clară în funcție de situație – de exemplu, dacă există un contact frecvent cu persoana în cauză, aceasta fiind, prin urmare, deja cunoscută (inclusiv adresa sa)[2].

[1] A se vedea, de asemenea, Souhrada-Kirchmayer, The right of access to the DSGVO, in Jahnel [Hrsg], Yearbook 17. Data Protection Law [2017] p86 și urm.
[2] A se vedea, de exemplu, jurisprudența Curților Supreme Austriece: VwGH 4.7.2016, Ra 2016/04/0014; OGH 25.2.1993, 6 Ob 6/93)

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

3.5. Costuri? Pot fi rambursate informațiile?

În principiu, informațiile trebuie furnizate gratuit (a se vedea articolul 12, alineatul (5) din RGPD). Cu toate acestea, în cazul cererilor vădit nefondate sau al solicitărilor excesiv repetate ale persoanei vizate, operatorul poate:

(a) să solicite o taxă rezonabilă, ținând seama de costurile administrative de notificare, comunicare sau punere în aplicare a măsurii solicitate; sau

b) să refuze soluționarea cererii.

3.6. Are solicitantul obligația de a participa la divulgarea informațiilor?

Da. Chiar dacă o obligație de cooperare este menționată numai în considerentul 63, în literatura de specialitate publicată până în prezent se presupune, în principal, că există (așa cum a fost recunoscut și în Austria în temeiul DSG 2000): „[î]n cazul în care operatorul prelucrează un număr mare de informații cu privire la persoana vizată, el ar trebui să poată solicita ca, înainte de furnizarea informațiilor, persoana vizată să precizeze ce informații sau activități de prelucrare fac obiectul cererii."[3]

3.7. Trebuie să fie luate în considerare drepturile terților atunci când sunt furnizate informații?

Da. Conform articolului 15, alineatul (4) din RGPD, dreptul de a obține o copie nu poate afecta drepturile și libertățile altora. În plus, considerentul 63 afirmă că *„[a]cest drept nu ar trebui să aducă atingere drepturilor sau libertăților altora, inclusiv secretului comercial sau proprietății intelectuale și, în special, drepturilor de autor care asigură protecția programelor software. Cu toate acestea, considerațiile de mai sus nu ar trebui să aibă drept rezultat refuzul de a furniza toate informațiile persoanei vizate."*

Prin urmare, este necesar să se controleze datele care trebuie divulgate, de regulă, datele cu caracter personal ale terților trebuie șterse din copia datelor (de exemplu, numele persoanei care figurează în fișierul clientului).

[3] Considerentul 63.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

4. Listă de verificare pentru divulgarea informațiilor la cerere

Sunt obligat să furnizez informații?	Dacă autoritatea publică locală este operator de prelucrare a datelor – DA. Dacă autoritatea publică locală este doar persoană împuternicită pentru prelucrarea datelor, însă primește totuși o solicitare, trebuie să o transmită imediat persoanei responsabile.
Verificare identității	Identitatea persoanei care solicită informațiile (persoana în cauză) trebuie să fie clară. Dacă aveți îndoieli cu privire la identitate, solicitați o dovadă.
Este gratuită divulgarea informațiilor?	În principiu – DA. Dacă solicitantului i s-au oferit aceleași informații de mai multe ori sau cererea afectează grav operatorul, poate fi percepută o taxă. NB! Această este și o chestiune de legislație națională. Prin urmare, verificați legislația aplicabilă la activitatea dumneavoastră.
Există date personale ale solicitantului care au fost prelucrate?	Dacă nu au fost stocate date despre solicitant sau dacă au fost șterse sau făcute anonime în mod ireversibil, datele cu caracter personal nu vor fi prelucrate și vor fi furnizate așa-numitele informații negative – „Nu vor fi prelucrate datele dumneavoastră cu caracter personal”.
Ce date și informații trebuie să furnizeze operatorul?	Trebuie furnizate toate datele stocate ale persoanei în cauză. În funcție de complexitatea sistemelor, trebuie luat în considerare în avans în ce categorii de baze de date pot fi găsite persoanele afectate. În plus, trebuie furnizate informațiile menționate la articolul 15, alineatul (1) din RGPD. Trebuie respectate drepturile terților (în special,

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

	secretele comerciale și datele terților trebuie șterse/înnegrite).

4.1. Emiterea informațiilor

Exemplu de divulgare a informațiilor în conformitate cu articolul 15 al RGPD

Cererea dumneavoastră de informații

Stimate Domnule / Stimată Doamnă [nume],

1. Cererea dumneavoastră din [data] cu privire la informații în temeiul art. 15 RGPD, primite de noi la [data], primește următorul răspuns:

2. [În cazul unui răspuns în termen de o lună de la primirea cererii] Prin prezenta, vă confirmăm din timp că prelucrăm date cu caracter personal despre dumneavoastră.

[În cazul prelungirii, în conformitate cu art. 12 (3) RGPD] După cum se menționează în scrisoarea din [data], ne-am permis să prelungim termenul până la trei luni din cauza [complexității cererii sau numărului de solicitări, explicații suplimentare necesare].

3. [Dacă nu sunt prelucrate date] Nu vor fi prelucrate datele dumneavoastră cu caracter personal. [Apoi continuați cu modulul de text nr.6].

[Dacă sunt prelucrate date] Mai precis, prelucrăm următoarele dumneavoastră date cu caracter personal: [aici apare lista datelor care urmează să fie prelucrate].

Printuri / copii ale prelucrărilor de date relevante pot fi găsite în anexă. Orice înnegrire sau omisiune a fost făcută astfel încât să nu afecteze drepturile și libertățile altora sau pentru că informațiile nu vă privesc.

4. [dacă datele nu au fost colectate de la persoana vizată]: Am obținut informațiile dumneavoastră de la [informații disponibile despre proveniența datelor - de exemplu, organismul public XY].

5. [Dacă este cazul] Vom utiliza proceduri automatizate de luare a deciziilor / profilare care au un efect juridic asupra dumneavoastră sau vă vor afecta într-un mod similar: [Vă rugăm să completați informații relevante despre logica implicată și despre consecințe].

6. Aveți dreptul la rectificare, ștergere, restricționare sau dreptul la anularea prelucrării datelor dumneavoastră cu caracter personal. Pentru mai multe detalii ne puteți contacta. În cazul în care considerați că prelucrarea datelor dumneavoastră încalcă legea privind protecția datelor sau dacă reclamațiile dumneavoastră privind protecția datelor au fost cumva încălcate, puteți să vă plângeți autorității de supraveghere. În această țară, XYZ este responsabil.

Cu stimă,

….

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

5. Bibliografie

5.1. Cărți și articole

- Souhrada-Kirchmayer, The right of access to the DSGVO, in Jahnel [Hrsg], Yearbook 17. Data Protection Law [2017] 86 f.
- ***Martini in Paal/Pauly*** (Ed.), Datenschutz-Grundverordnung (2016).

5.2. Alte documente și cazuri

- Jurisprudența Curților Supreme Austriece: VwGH 4.7.2016, Ra 2016/04/0014; OGH 25.2.1993, 6 Ob 6/93) Web Links
- Pentru a compara modificările aduse directivei 95/46/CE, a se vedea https://gdpr.report/news/2017/11/20/gdpr-subject-access-requests/

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

ProLegis

Právne dôvody na spracovanie osobných údajov

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

Contents

1. PRÁVNY RÁMEC 3

1.1. Charta základných práv EU 3

1.2. GDPR 3

2. PRÁVNYN RÁMEC PRE SPRACOVANIA OSOBNÝCH ÚDAJOV PODĽA GDPR 9

2.1. Súhlas 9

2.1.1. Význam a právne požiadavky 9

2.1.2. Uplatniteľnosť v kontexte činnosti Miestnych orgánov 11

2.2. Vykonávanie / uzatvorenie zmluvy s dotknutou osobou 12

2.2.1. Význam a právne požiadavky 12

2.2.2. Uplatniteľnosť v kontexte činnosti miestnych orgánov 13

2.3. Právne nariadenia 14

2.3.1. Význam a právne požiadavky 14

2.3.2. Uplatniteľnosť v kontexte činnosti miestnych orgánov 15

2.4.1. Význam a právne požiadavky 15

2.4.2. Uplatniteľnosť v kontexte činnosti Miestnych orgánov 16

2.5. Úloha vykonávaná vo verejnom záujme – výkon úradnej moci 16

2.5.1. Význam a právne požiadavky 16

2.5.2. Uplatniteľnosť v kontexte činnosti Miestnych orgánov 17

2.6. Právne záujmy 17

2.6.1. Význam a právne požiadavky 17

2.6.2. Uplatniteľnosť v kontexte činnosti Miestnych orgánov 18

3. Záver a Praktické rady 19

4. Externé zdroje a webové stránky 19

Knihy 19

Dokumenty článku 29 19

Web Links 20

5. REFERENCIE 20

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

1. PRÁVNY RÁMEC

1.1. Charta základných práv EU

Článok 8

Ochrana osobných údajov

1. Každý má právo na ochranu osobných údajov, ktoré sa ho týkajú.

2. Tieto údaje musia byť riadne spracované na určené účely ***na základe súhlasu dotknutej osoby alebo na inom oprávnenom základe ustanovenom zákonom.*** *Každý má právo na prístup k zhromaždeným údajom, ktoré sa ho týkajú, a právo na ich opravu*

3. Dodržiavanie týchto pravidiel podlieha kontrole nezávislého orgánu

1.2. GDPR

Recitál (42)

[…] Aby bol súhlas informovaný, dotknutá osoba by mala byť informovaná aspoň o totožnosti kontrolóra a o účeloch spracovania, pre ktoré sú osobné údaje určené. Súhlas by sa nemal považovať za slobodne poskytnutý, ak dotknutá osoba nemá skutočnú alebo slobodnú voľbu, alebo nie je schopná odmietnuť alebo odobrať súhlas bez ujmy.

Recitál (43) Interpretácia -

Aby sa zabezpečilo, že súhlas sa poskytol slobodne, súhlas by nemal byť platným právnym dôvodom na spracúvanie osobných údajov v konkrétnom prípade, ak medzi postavením dotknutej osoby a prevádzkovateľa existuje jednoznačný nepomer, najmä ak je prevádzkovateľ orgánom verejnej moci, a preto nie je pravdepodobné, že sa súhlas poskytol slobodne za všetkých okolností danej konkrétnej situácie. Súhlas sa nepovažuje za poskytnutý slobodne, ak nie je možné dať samostatný súhlas na jednotlivé spracovateľské operácie osobných údajov napriek tomu, že by to bolo v konkrétnom prípade vhodné, alebo ak sa plnenie zmluvy vrátane poskytnutia služby podmieňuje takýmto súhlasom, aj keď to na takéto plnenie nie je takýto súhlas nevyhnutný.

Recitál (44)

> *Spracúvanie by sa malo považovať za zákonné, ak* ***je potrebné v súvislosti so zmluvou alebo s úmyslom uzatvoriť zmluvu****.*

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

Recitál (45)

*Ak sa spracúvanie vykonáva v súlade so **zákonnými povinnosťami**, ktoré má prevádzkovateľ, alebo ak je spracúvanie potrebné na splnenie úlohy realizovanej vo verejnom záujme alebo z úradnej moci, základ pre spracúvanie by mal existovať v práve Únie alebo v práve členského štátu. Týmto nariadením sa nevyžaduje, aby pre každé jednotlivé spracúvanie existoval osobitný právny predpis. Za dostatočný možno považovať právny predpis, ktorý je základom pre viaceré spracovateľské operácie založené na zákonnej povinnosti, ktorá sa vzťahuje na prevádzkovateľa, alebo ak je spracúvanie nevyhnutné na splnenie úlohy realizovanej vo verejnom záujme alebo pri výkone verejnej moci. Na základe práva Únie alebo práva členského štátu by sa tiež malo rozhodovať o účele spracúvania. Okrem toho by toto právo mohlo spresniť všeobecné podmienky tohto nariadenia, ktoré sa týkajú zákonnosti spracúvania osobných údajov, stanoviť špecifikácie na určenie prevádzkovateľa, typu osobných údajov, ktoré podliehajú spracúvaniu, príslušných dotknutých osôb, subjektov, ktorým môžu byť osobné údaje poskytnuté, obmedzenia účelu, doby uchovávania a iných opatrení s cieľom zabezpečiť zákonné a spravodlivé spracúvanie. V práve Únie alebo v práve členského štátu by malo byť takisto stanovené, či by prevádzkovateľom vykonávajúcim úlohu vo verejnom záujme alebo pri výkone verejnej moci mal byť orgán verejnej moci alebo iná fyzická alebo právnická osoba, ktorá sa spravuje verejným alebo súkromným právom, ako napríklad profesijné združenie, ak je to z dôvodu verejného záujmu opodstatnené, a to aj na účely v oblasti zdravia, ako je verejné zdravie a sociálna ochrana a správa služieb zdravotnej starostlivosti.*

Recitál (46)

*Spracúvanie osobných údajov by sa malo rovnako považovať za zákonné, ak je potrebné na účely ochrany záujmu, **ktorý je zásadný pre život dotknutej alebo inej fyzickej osoby**. Spracúvanie osobných údajov na základe životne dôležitom záujme inej fyzickej osoby by sa malo uskutočniť v zásade len vtedy, keď sa takéto spracúvanie zjavne nemôže zakladať na inom právnom základe. Niektoré typy spracúvania môžu slúžiť na dôležité účely verejného záujmu aj životne dôležité záujmy dotknutej osoby, napríklad ak je spracúvanie nevyhnutné na humanitárne účely vrátane monitorovania epidémií a ich šírenia alebo v humanitárnych núdzových situáciách, najmä v prípade prírodných katastrof a katastrof spôsobených ľudskou činnosťou.*

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

Recitál (47)

***Oprávnené záujmy prevádzkovateľa vrátane prevádzkovateľa, ktorému môžu byť tieto osobné údaje poskytnuté, alebo tretej stran**y môžu poskytnúť právny základ pre spracúvanie, ak nad nimi neprevažujú záujmy alebo základné práva a slobody dotknutej osoby, pričom sa zohľadnia primerané očakávania dotknutých osôb na základe ich vzťahu k prevádzkovateľovi. Takýto oprávnený záujem by mohol existovať napríklad vtedy, keby medzi dotknutou osobou a prevádzkovateľom existoval relevantný a primeraný vzťah, napríklad keby bola dotknutá osoba voči prevádzkovateľovi v postavení klienta alebo v jeho službách. Existencia oprávneného záujmu by si v každom prípade vyžadovala dôkladné posúdenie vrátane posúdenia toho, či dotknutá osoba môže v danom čase a kontexte získavania osobných údajov primerane očakávať, že sa spracúvanie na tento účel môže uskutočniť. Záujmy a základné práva dotknutej osoby by mohli prevážiť nad záujmami prevádzkovateľa údajov najmä vtedy, ak sa osobné údaje spracúvajú za okolností, keď dotknuté osoby primerane neočakávajú ďalšie spracúvanie. Keďže je úlohou zákonodarcu, aby v právnych predpisoch stanovil právny základ pre spracúvanie osobných údajov orgánmi verejnej moci, tento právny základ by sa nemal vzťahovať na spracúvanie orgánmi verejnej moci pri plnení ich úloh. Spracúvanie osobných údajov nevyhnutne potrebné na účely predchádzania podvodom tiež predstavuje oprávnený záujem príslušného prevádzkovateľa údajov. Spracúvanie osobných údajov na účely priameho marketingu možno považovať za oprávnený záujem.*

Recitál (48)

Prevádzkovatelia, ktorí sú súčasťou skupiny podnikov alebo inštitúcií, ktoré sú prepojené s ústredným subjektom, môžu mať oprávnený záujem na prenose osobných údajov v rámci skupiny podnikov na vnútorné administratívne účely vrátane spracúvania osobných údajov klientov alebo zamestnancov. Tým nie sú dotknuté všeobecné zásady prenosu osobných údajov v rámci skupiny podnikov podniku nachádzajúcemu sa v tretej krajine.

Recitál (49)

Spracúvanie osobných údajov v rozsahu nevyhnutne potrebnom a primeranom na účely zaistenia bezpečnosti siete a informačnej bezpečnosti, t. j. schopnosti siete alebo informačného systému odolať na danom stupni dôvernosti poruchám alebo nezákonným alebo úmyselným činom, ktoré narušujú dostupnosť, pravosť, integritu a dôvernosť uchovávaných alebo prenesených osobných údajov, a bezpečnosti súvisiacich služieb ponúkaných alebo dostupných prostredníctvom týchto sietí a systémov orgánmi verejnej moci, jednotkami reakcie na núdzové počítačové situácie (CERT), jednotkami pre riešenie počítačových incidentov

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

(CSIRT), poskytovateľmi elektronických komunikačných sietí a služieb a poskytovateľmi bezpečnostných technológií a služieb predstavuje oprávnený záujem

dotknutého prevádzkovateľa údajov. Mohlo by to napríklad zahŕňať zabránenie neoprávnenému prístupu k elektronickým komunikačným sieťam a šíreniu škodlivých programových kódov, ako aj zastavenie útokov sledujúcich cielené preťaženie serverov („denial of service“) a poškodzovanie počítačových a elektronických komunikačných systémov.

.

Recitál (50)

Spracúvanie osobných údajov na iné účely ako na účely, na ktoré boli osobné údaje pôvodne získané, by malo byť umožnené len vtedy, ak je toto spracúvanie zlučiteľné s účelmi, na ktoré boli osobné údaje pôvodne získané. V takom prípade sa nevyžaduje žiadny iný samostatný právny základ, než je právny základ, ktorý umožňoval získavanie osobných údajov. Ak je spracúvanie potrebné na splnenie úlohy realizovanej vo verejnom záujme alebo pri výkone verejnej moci zverenej prevádzkovateľovi, v práve Únie alebo v práve členského štátu sa môžu stanoviť a upraviť úlohy a účely, v prípade ktorých by sa malo ďalšie spracúvanie považovať za zlučiteľné a zákonné. Ďalšie spracúvanie na účely archivácie vo verejnom záujme, na účely vedeckého či historického výskumu alebo štatistické účely by sa malo považovať za zlučiteľné so zákonnými spracovateľskými operáciami. Právny základ pre spracúvanie osobných údajov, ktorý je zakotvený v práve Únie alebo v práve členského štátu, môže byť aj právnym základom pre ďalšie spracúvanie. S cieľom zistiť, či je účel ďalšieho spracúvania v súlade s účelom, na ktorý boli osobné údaje pôvodne získané, by mal prevádzkovateľ po splnení všetkých požiadaviek zákonnosti pôvodného spracúvania zohľadniť okrem iného akékoľvek prepojenie medzi týmito účelmi a účelmi zamýšľaného ďalšieho spracúvania; kontext, v ktorom sa osobné údaje získali, najmä primerané očakávania dotknutých osôb vyplývajúce z ich vzťahu k prevádzkovateľovi, pokiaľ ide o ich ďalšie použitie; povahu osobných údajov; následky zamýšľaného ďalšieho spracúvania pre dotknuté osoby; a existenciu primeraných záruk v pôvodných aj zamýšľaných operáciách ďalšieho spracúvania.

Ak dotknutá osoba udelila súhlas alebo sa spracúvanie zakladá na práve Únie alebo práve členského štátu, ktoré predstavuje potrebné a primerané opatrenie v demokratickej spoločnosti, najmä na ochranu dôležitých verejných záujmov, mal by mať prevádzkovateľ možnosť osobné údaje ďalej spracúvať bez ohľadu na

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

zlučiteľnosť účelov. V každom prípade by sa malo zabezpečiť uplatnenie zásad stanovených v tomto nariadení, najmä povinnosti informovať dotknutú osobu o týchto iných účeloch a o jej právach vrátane práva namietať. Oznámenie možných trestných činov alebo ohrozenia verejnej bezpečnosti prevádzkovateľom a poskytnutie relevantných osobných údajov v jednotlivých prípadoch alebo viacerých prípadoch týkajúcich sa toho istého trestného činu alebo ohrozenia verejnej bezpečnosti príslušnému orgánu by sa malo považovať za oprávnený záujem, ktorý sleduje prevádzkovateľ. Takéto poskytnutie v oprávnenom záujme prevádzkovateľa alebo ďalšie spracúvanie osobných údajov by sa však malo zakázať, ak toto spracúvanie nie je v súlade s právnou, profesijnou alebo inou záväznou povinnosťou mlčanlivosti.

Článok 4

Definície

Na účely tohto nariadenia:

[…]

(11) „súhlas dotknutej osoby " je akýkoľvek ***slobodne daný, konkrétny, informovaný a jednoznačný prejav vôle dotknutej osoby, ktorým formou vyhlásenia alebo jednoznačného potvrdzujúceho úkonu vyjadruje súhlas so spracúvaním osobných údajov, ktoré sa jej týka****;*

Článok 6

Zákonnosť spracúvania

1. *Spracúvanie je zákonné iba vtedy a iba v tom rozsahu, keď je splnená aspoň jedna z týchto podmienok:*

a) *dotknutá osoba vyjadrila súhlas so spracúvaním svojich osobných údajov na* ***jeden alebo viaceré konkrétne účely****;*

b) *spracúvanie je nevyhnutné na splnenie zmluvy, ktorej zmluvnou stranou je dotknutá osoba, alebo aby sa na základe žiadosti dotknutej osoby vykonali opatrenia pred*

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

uzatvorením zmluvy;

spracúvanie je nevyhnutné na splnenie zákonnej povinnosti prevádzkovateľa;

c) *spracúvanie je nevyhnutné, aby sa ochránili životne dôležité záujmy dotknutej osoby alebo inej fyzickej osoby;*

d) *spracúvanie je nevyhnutné na splnenie úlohy realizovanej vo verejnom záujme alebo pri výkone verejnej moci zverenej prevádzkovateľovi;*

e) *spracúvanie je nevyhnutné na účely oprávnených záujmov, ktoré sleduje prevádzkovateľ alebo tretia strana, s výnimkou prípadov, keď nad takýmito záujmami prevažujú záujmy alebo základné práva a slobody dotknutej osoby, ktoré si vyžadujú ochranu osobných údajov, najmä ak je dotknutou osobu dieťa.*

Bod f) prvého pod odseku sa nevzťahuje na spracúvanie vykonávané orgánmi verejnej moci pri výkone ich úloh.

Členské štáty môžu zachovať alebo zaviesť špecifickejšie ustanovenia s cieľom prispôsobiť uplatňovanie pravidiel tohto nariadenia s ohľadom na spracúvanie v súlade s odsekom 1 písm. c) a e), a to presnejším stanovením osobitných požiadaviek na spracúvanie a stanovením ďalších opatrení, ktorými sa zaistí zákonné a spravodlivé spracúvanie, vrátane požiadaviek na iné osobitné situácie spracúvania stanovené v kapitole IX.

2. Základ pre spracúvanie uvedené v odseku 1 písm. c) a e) musí byť stanovený:
a) v práve Únie alebo
b) v práve členského štátu vzťahujúcom sa na prevádzkovateľa.

Účel spracúvania sa stanoví v tomto právnom základe, alebo pokiaľ ide o spracúvanie uvedené v odseku 1 písm. e), spracúvanie je nevyhnutné na splnenie úlohy realizovanej vo verejnom záujme alebo pri výkone verejnej moci zverenej prevádzkovateľovi. Uvedený právny základ môže obsahovať osobitné ustanovenia na prispôsobenie uplatňovania pravidiel tohto nariadenia, vrátane: všeobecných podmienok vzťahujúcich sa na zákonnosť spracúvania prevádzkovateľom; typov spracúvaných údajov; dotknutých osôb; subjektov, ktorým sa môžu osobné údaje poskytnúť, a účely, na ktoré ich možno poskytnúť; obmedzenia účelu; doby uchovávania; a spracovateľských operácií a postupov vrátane opatrení na zabezpečenie zákonného a spravodlivého spracúvania, ako napríklad tie na iné osobitné situácie spracúvania, ako sú stanovené v kapitole IX. Právo Únie alebo

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

právo členského štátu musí spĺňať cieľ verejného záujmu a byť primerané sledovanému oprávnenému cieľu.

3. Ak spracúvanie na iné účely ako na účely, na ktoré boli osobné údaje získavané, nie je založené na súhlase dotknutej osoby alebo na práve Únie alebo práve členského štátu, ktoré predstavuje potrebné a primerané opatrenie v demokratickej spoločnosti na ochranu cieľov uvedených v článku 23 ods. 1, prevádzkovateľ na zistenie toho, či je spracúvanie na iný účel zlučiteľné s účelom, na ktorý boli osobné údaje pôvodne získané, okrem iného zohľadní:

a) akékoľvek prepojenie medzi účelmi, na ktoré sa osobné údaje získali, a účelmi zamýšľaného ďalšieho spracúvania;

b) okolnosti, za akých sa osobné údaje získali, najmä týkajúce sa vzťahu medzi dotknutými osobami a prevádzkovateľom;

c) povahu osobných údajov, najmä či sa spracúvajú osobitné kategórie osobných údajov podľa článku 9 alebo osobné údaje týkajúce sa uznania viny za trestné činy a priestupky podľa článku 10;

d) možné následky zamýšľaného ďalšieho spracúvania pre dotknuté osoby;

e) existenciu primeraných záruk, ktoré môžu zahŕňať šifrovanie alebo pseudonymizáciu.

2. PRÁVNYN RÁMEC PRE SPRACOVANIA OSOBNÝCH ÚDAJOV PODĽA GDPR

2.1. Súhlas

2.1.1. Význam a právne požiadavky

Súhlas dotknutej osoby je akýkoľvek slobodne daný, konkrétny, informovaný a jednoznačný prejav vôle dotknutej osoby, ktorým formou vyhlásenia alebo jednoznačného potvrdzujúceho úkonu vyjadruje súhlas so spracúvaním jej osobných údajov.“.

- **slobodne daný’** = znamená skutočnú voľbu a kontrolu pre dotknuté osoby. Ak sa vyskytnú akékoľvek nepriaznivé následky pre dotknutú osobu v prípade, že nesúhlasí so spracovaním/ odvolaním už udeleného súhlasu (napr. odmietnutie

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

služby, vyššie náklady na tovar/službu - poplatky, cena, atď.). Vzhľadom na nerovnováhu právomocí medzi orgánmi verejnej moci a dotknutými osobami by sa súhlas mal zriedka považovať za užitočný nástroj na spracovanie údajov v kontexte výkonu úradných orgánov;

- **‘špecifický’** = úzko súvisí s požiadavkou, aby dotknutá osoba súhlasila s jedným alebo viacerými konkrétnymi účelmi spracovania (tzv. granularita súhlasu) a s účelom špecifikácie princípu/pravidla. Každý z účelov spracovania údajov musí byť jasne definovaný od začiatku pred dotknutou osobou. Dotknutá osoba by mala mať možnosť vybrať si na aké účely dáva súhlas (napr. súhlas s účelom A, B a C a nesúhlas s účelom E a D). Informácie týkajúce sa súhlasu by mali byť jasne oddelené od informácií, ktoré súvisia s inými záležitosťami. Musí sa získať súhlas na akýkoľvek nový účel spracovania a kontrolóri by mali poskytnúť špecifické informácie o údajoch s každou samostatnou žiadosťou o súhlas, ktoré sa spracúvajú na každý konkrétny účel

- **‘informovaný** = minimálne požiadavky podľa GDPR zahŕňajú poskytovanie informácií pre správcu údajov a účely spracovania. Pracovná skupina zriadená podľa článku 29 (WP29) odporúča zakomponovať dodatočné informácie, ako napríklad typ zozbieraných a používaných údajov; právo odobrať súhlas; informácie o využívaní údajov na rozhodnutia založené výlučne na automatizovanom spracovaní vrátane profilovania; v prípade prevodov - informácie o možných rizikách prenosu údajov do tretích krajín bez rozhodnutia o adekvátnosti a primeraných záruk[i].
- **‘jednoznačný’** = súhlas musí byť poskytnutý prostredníctvom vyhlásenia dotknutej osoby, alebo jasného **pozitívneho**/potvrdzujúceho úkonu. Súhlas sa musí vždy poskytnúť aktívnym návrhom alebo vyhlásením. Teda, prázdne, predznačené políčka a nečinnosť nemôžu predstavovať platný súhlas podľa GDPR;

- **As easily withdrawn as given** = súhlas by mohol byť kedykoľvek zrušený. Nemalo by to nevyhnutne prebiehať súčinne s tou istou aktivitou, ale proces odvolania by mal byť taký jednoduchý ako proces udeľovania súhlasu (napríklad kliknutím na políčko v online vyhlásení o súhlase s prijatím novín obce je rovnako jednoduché ako kliknutie na odkaz v tele e-mailu, ktoré sprevádza newsletter na odhlásenie a odobratie súhlasu);
- **Špecifické požiadavky udelenia súhlasu od dieťaťa** =GDPR považuje deti za zraniteľnú kategóriu dotknutých osôb. Preto si zaslúžia osobitnú ochranu, keďže si nemôžu byť vedomí všetkých dotknutých rizík, dôsledkov a záruk ako aj ich práv

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

v súvislosti so spracovaním osobných údajov. V prípade poskytovania služieb informačnej spoločnosti ponúkaných dieťaťu (napr. on-line vzdelávacie kampane realizované na webových stránkach obcí, ktoré vyžadujú zber osobných údajov detí), súhlas na spracovanie údajov detí do 16 rokov (členské štáty môžu znížiť toto vek do 13 rokov) by mal byť získaný od oprávnenej osoby – v zmysle zákonnej zodpovednosti nad dieťaťom;

- **Súhlas v zmysle Nariadenia 95/46** = už získaný súhlas v rámci starého režimu nemusí byť nevyhnutne revidovaný. Ak súhlas zodpovedá požiadavkám stanoveným v GDPR, potom súhlas získaný podľa smernice by mal naďalej zostať platným dôvodom na spracovanie.

Správca údajov má dôkazné bremeno na preukázanie, že súhlas bol riadne získaný.

2.1.2. Uplatniteľnosť v kontexte činnosti Miestnych orgánov

V praxi súhlas zriedka predstavuje základný právny základ, podľa ktorého miestne orgány (MO) budú oprávnene spracúvať osobné údaje občanov. Tento záver vyplýva z požiadaviek GDPR, ktoré musí súhlas spĺňať, aby nadobudli platnosť.

Po prvé, skutočnosť, že súhlas by mal byť "slobodne poskytnutý", znamená, že dotknutá osoba by nemala trpieť nepriaznivými dôsledkami v prípade, že neposkytne daný súhlas, znamená to, že v každej situácii, v ktorej konkrétne MO koná ako držiteľ/reprezentant verejnej moci, nemožno použiť ako platný právny základ na spracovanie. Kontrola riadneho plnenia verejných povinností občanov (napr. zhromažďovanie miestnych poplatkov a daní, evidenciu nadobudnutia nehnuteľností / vozidiel atď.) a uloženie sankcií v prípade nesplnenia týchto povinností je neodmysliteľne spojená s právom (a povinnosťou) vykonávať vynucovacie právomoci. Znamená to, že dotknuté osoby nemajú skutočnú slobodnú vôľu súhlasiť alebo nesúhlasiť so súhlasom na spracovanie svojich osobných údajov. Sú v podriadenom postavení a sú zo zákona povinné spolupracovať s MO.

Po druhé, súhlas by mohol byť kedykoľvek zrušený. Ak bol súhlas oprávneným dôvodom na spracovanie osobných údajov v prípade, že občania plnia svoje zákonné povinnosti, potenciálny občan, ktorý nekoná v **dobrej** viere (napr. nie je ochotný plniť určitú verejnú povinnosť), by mohol kedykoľvek stiahnuť svoj súhlas a mohol využiť toto stiahnutie na vytváranie prekážok (a v praxi "blokovať") normálne fungovanie MO. Ak je súhlas odňatý, MO ako kontrolór údajov by mal spracovanie ukončiť. To je nemysliteľné v prípade výkonu úradných orgánov, pretože to ohrozí celú myšlienku výkonu verejnej moci.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

Preto, v situáciách uvedených vyššie, súhlas nie je správnym nástrojom na takéto spracovanie.

Podľa WP29 "*používanie súhlasu ako zákonného základu pre spracovanie údajov verejnými orgánmi* **nie je úplne vylúčené** z právneho rámca GDPR". **Takýto** súhlas by mohol byť užitočným nástrojom v situáciách, v ktorých MO nevykonáva svoje štandardné a hlavné funkcie, alebo konkrétne spracovanie je skôr voliteľné (a existujú štandardné postupy spracovania, ktoré sa uskutočnia v prípade, že dotknutá osoba nesúhlasí). Príkladmi sú nasledujúce situácie:

- MO a štátne orgány vyžadujú na požiadanie občana rovnaké informácie na vydávanie určitého právneho aktu, ale nemôžu mať prístup k databázam druhej strany. Keď obe inštitúcie žiadajú občanov o rovnaké informácie, mohli by požiadať o súhlas občana, aby zlúčili spisy, aby sa vyhli duplicitným postupom a korešpondencii. Obidva verejné orgány by mali zabezpečiť voliteľnosť takéhoto úkonu a vydávanie dokladu zabezpečiť aj vtedy, ak by občan nesúhlasil so zlúčením údajov[ii];
- MO ustanovuje možnosť informovať občanov, ktorí sa zúčastňujú na správnom konaní pred nimi, prostredníctvom e-mailu. Režim je povolený, t. j. občania sa môžu slobodne rozhodnúť, či sa notifikujú prostredníctvom e-mailu (napríklad zaškrtnutím políčka v online / papierovom formulári a poskytnutím ich e-mailu). V prípade odmietnutia súhlasu / odstúpenia od súhlasu by MO mal mať predvolený postup na oznamovanie (napríklad doporučenou poštou). Spracovanie e-mailu v takom prípade by bolo založené na súhlase;
- MO poskytuje občanom možnosť predplatiť si pozvánky na rôzne aktivity organizované MO (napr. výstavy v miestnych múzeách, premiéry divadla v obci, kampane na zhromažďovanie odpadu, súťaže/ vzdelávacie kampane realizované v školách obce). Predplatné vyžaduje poskytnutie kontaktných údajov (ako napríklad adresa, telefónne číslo, e-mail atď.), ako aj údaje o preferenciách dotknutých osôb (napríklad záľuby, záujmy atď.). Spracovanie takýchto údajov by bolo založené na súhlase a občania ba mali právo kedykoľvek zrušiť takéto upozornenia a to bez postihu/ujmy.

2.2. Vykonávanie / uzatvorenie zmluvy s dotknutou osobou

2.2.1. Význam a právne požiadavky

Ustanovenie čl. 6, odsek 1, písmeno "b" GDPR zavádza dva samostatné právne základy na spracovanie osobných údajov:

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

(i) spracúvanie *je nevyhnutné na plnenie zmluvy, ktorej zmluvnou stranou je dotknutá osoba, alebo aby sa na základe žiadosti dotknutej osoby vykonali opatrenia pred uzatvorením zmluvy;*

(ii) spracúvanie *je nevyhnutné na splnenie zákonnej povinnosti prevádzkovateľa* Týka sa to predzmluvných vzťahov za predpokladu, že na žiadosť dotknutej osoby sa podniknú kroky, a nie na podnet kontrolóra alebo akejkoľvek tretej strany.

Prvá hypotéza by sa mala vykladať striktne a nemala by sa vzťahovať na situácie, kedy spracovanie nie je skutočne nevyhnutné pre plnenie zmluvy, **ale je dotktnutou osobou jednostranne uložené prevádzkovateľom/kontrolórom.** Podľa výkladu, ktorý dodala WP29 z rovnakého dôvodu podľa staršej smernice 95/46, uvedený právny dôvod sa vzťahuje len na to, čo je nevyhnutné pre výkon zmluvy. Inými slovami, pokiaľ sa spracovanie vzťahuje na bežné plnenie zmluvy, mohlo by to spadať do uvedeného právneho základu.

Tento právny dôvod by sa vzťahoval na situácie, kedy sa spracovanie uskutočňuje v rámci zmluvy bez ohľadu na to, v ktorej fáze sa zmluva nachádza. Akékoľvek ďalšie opatrenia, ktoré boli vyvolané/spôsobené nesúladom alebo inými mimoriadnymi udalosťami pri plnení zmluvy, však nepatria do rozsahu tohto právneho dôvodu. Takéto spracovanie by si vyžadovalo aplikáciu rôznych právnych dôvodov - napr. nadradený legitímny záujem správcu údajov.

Druhá hypotéza by mohla zahŕňať spracovanie potrebné na prípravu ponúk, prijímanie do zamestnania v oblasti ľudských zdrojov, atď. Avšak všetky podrobné overovania uchádzačov by boli dosť rozsiahle a neboli by to opodstatnené kroky požadované dotknutou osobou.

Vo všeobecnosti sa tento právny dôvod interpretuje len regulačnými orgánmi, takže prevádzkovatelia by mali byť schopní preukázať, že spracovanie je nevyhnutné na dokončenie zmluvy[iii].

2.2.2. Uplatniteľnosť v kontexte činnosti miestnych orgánov

Tento právny dôvod na spracovanie osobných údajov by mal byť uplatňovaný miestnymi orgánmi aspoň v týchto oblastiach:

- *Spracovanie v kontexte zamestnania - napríklad spracovanie informácií o mzdách a podrobnosti o bankovom účte, aby sa mohli vyplácať mzdy [iv];*
- Spracovanie v kontexte uzatvárania zmlúv o verejnom obstarávaní - tento zmluvný právny základ by sa mohol prekrývať s iným právnym základom na spracovanie osobných údajov - napr. právna povinnosť MO na spracovanie

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

osobných údajov v rámci príslušného správneho konania stanoveného miestnym zákonom;

- spracovanie v kontexte vzťahov medzi niektorými súkromnými subjektmi, ktoré sú v úplnom/ čiastočnom vlastníctve obce/ štátu a občanov - napr. subjekty poskytujúce služby verejnej dopravy v rámci celého mesta/obce, subjekty poskytujúce verejnoprospešné služby (elektrina, plyn, zásobovanie vodou atď.) pri uzatváraní príslušných zmlúv.

2.3. Právne nariadenia

2.3.1. Význam a právne požiadavky

Tento právny základ si vyžaduje jasné právne ustanovenie, ktoré sa zavádza buď na legislatívnej alebo na sub-legislatívnej úrovni (tzv. sekundárna legislatíva niektorých členských štátov), ktorá zaväzuje prevádzkovateľa vykonávať spracovanie. WP29 zdôrazňuje, že zákon musí spĺňať všetky príslušné podmienky na to, aby záväzok bol platný a záväzný, a musí tiež dodržiavať zákony na ochranu údajov vrátane požiadavky nevyhnutnosti, proporcionality a obmedzenia účelu. V GDPR sa výslovne vyžaduje, aby táto povinnosť bola kumulatívna:

(i) Povinnosti členského štátu alebo práva EÚ, ktorému podlieha prevádzkovateľ. WP29 už v tomto smere vykonával podľa staršej smernice 95/46 tento výklad: povinnosti vyplývajúce zo zákonov tretích krajín (napríklad povinnosť zriadiť systémy oznamovania podľa zákona Sarbanes-Oxley z roku 2002 v Spojených štátoch) nie sú kryté základnou právnou povinnosťou. Aby bol právny záväzok tretej krajiny platný, musí byť úradne uznaný a začlenený do právneho poriadku príslušného členského štátu, napr. vo forme medzinárodnej dohody; a

(ii) „ jasné a presné“ a jeho uplatňovanie je predvídateľné pre tých, ktorých sa to týka. Odôvodnenia 41 a 45 GDPR jasne uvádzajú, že príslušná "právna povinnosť" nemusí byť zákonná, čo by mohlo mať praktické dôsledky pre krajiny s bežným právom - bolo by dostatočné, ak by to spĺňalo "jasný a presný" test. Právna povinnosť by mohla zahŕňať niekoľko operácií spracovania vykonávaných prevádzkovateľom, aby nebolo potrebné určiť konkrétnu právnu povinnosť pre každú jednotlivú spracovateľskú činnosť [v]

WP29 uviedla, že na to, aby sa mohol tento právny dôvod uplatniť, prevádzkovateľ nemôže mať možnosť rozhodnúť sa, či splní alebo nesplní svoju povinnosť. Dobrovoľné

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

jednostranné záväzky a partnerstvá verejného a súkromného sektora, ktoré spracúvajú údaje nad rámec zákona, nie sú týmto právnym základom pokryté. Právna povinnosť ako dôvod na spracovanie osobných údajov by sa mala uplatňovať na základe právnych ustanovení výslovne odkazujúcich na povahu a predmet spracovania. Prevádzkovateľ by nemal mať neprimeraný stupeň slobodnej úvahy o tom, ako dodržať zákonnú povinnosť[vi].

WP29 explicitne uznáva, že právne predpisy môžu v niektorých prípadoch stanoviť len všeobecný cieľ, zatiaľ čo špecifickejšie povinnosti sa ukladajú na inej úrovni (napríklad v sekundárnych právnych predpisoch alebo záväznom rozhodnutí verejného orgánu). Podľa WP29 to môže viesť aj k právnym povinnostiam za predpokladu, že charakter a predmet spracovania sú dobre definované a podliehajú primeranému právnemu základu[vii].

2.3.2. Uplatniteľnosť v kontexte činnosti miestnych orgánov

V praxi by tento právny základ bol jedným z najdôležitejších právnych dôvodov na spracovanie osobných údajov vykonávaných orgánmi verejnej správy. Tento právny základ by sa vzťahoval na obe situácie týkajúce sa poskytovania administratívnych služieb / uľahčenia plnenia verejných záväzkov občanov a plnenia určitých osobitných povinností orgánov územnej samosprávy ako zamestnávateľov. Tento právny základ by sa mohol uplatňovať napr. v týchto situáciách:

- zhromažďovanie údajov MO na spracovanie sankcií za parkovanie na nepovolaných miestach;
- vykazovanie platových údajov zamestnancov MO sociálnemu zabezpečeniu alebo daňovým úradom [viii].

2.4. Životne dôležitý záujem

2.4.1. Význam a právne požiadavky

Tento právny dôvod sa má vykladať veľmi úzko, WP29 tiež uznal, že životne dôležitý záujem by mal mať obmedzenú aplikáciu. Pojem "životne dôležitý záujem" je neodmysliteľne spojený s bezprostredným ohrozením základných tovarov dotknutej osoby (život, integrita tela atď.) V právnej doktríne sa uvádza, že plánované spracovanie by malo byť životne dôležité pre prežitie jednotlivca Podľa výkladu WP29 podľa staršej smernice 95/46 by hrozba mala byť okamžitá, t.j. zber a spracovanie osobných údajov vo veľkom rozsahu z čisto preventívnych dôvodov nemôže spadať do rozsahu pôsobnosti tohto právneho základu. V odôvodnení č. 46 GDPR sa výslovne povoľuje spracovanie na tomto právnom základe na humanitárne účely vrátane monitorovania epidémií a ich šírenia alebo v situáciách humanitárnych núdzových situácií, v situáciách prírodných a

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

človekom spôsobených katastrof (v týchto scenároch sa môže prekrývať s oboma dôležitými dôvodov verejného záujmu a životného záujmu). Preto by táto striktná interpretácia uložená WP29 mohla byť v budúcnosti "zmäkčená".

Treba tiež poznamenať, že podľa staršej smernice 95/46 sa právny dôvod "životného záujmu" týkal iba záujmov dotknutej osoby. V prípade GDPR má rozsah tohto právneho rámca širší rozsah - životný záujem by mohol byť buď subjekt údajov, alebo iná fyzická osoba. GDPR výslovne požaduje, aby spracovanie osobných údajov založené na životnom záujme inej fyzickej osoby sa v zásade uskutočňovalo len vtedy, ak sa spracovanie nemôže zakladať na inom právnom základe. Inými slovami, založenie spracovania na životne dôležitom záujme by bolo skôr riešením "poslednej inštancie" pre prevádzkovateľov.

2.4.2. Uplatniteľnosť v kontexte činnosti Miestnych orgánov

Možnosť uplatniť tento dôvod v kontexte aktivít MO je dosť obmedzená. Tento právny základ by teoreticky mohol byť použitý vo veľmi obmedzenom počte prípadov, napr. ospravedlniť spracovanie osobných údajov zamestnancov alebo občanov v prípade mimoriadnych udalostí, ku ktorým došlo v rámci jurisdikcie MO, a ak neexistuje iný právny dôvod na takéto spracovanie (napríklad právna povinnosť alebo vykonávanie verejnej moci).

2.5. Úloha vykonávaná vo verejnom záujme – výkon úradnej moci

2.5.1. Význam a právne požiadavky

Úloha alebo právomoc správcu údajov by sa mali stanoviť v právnych predpisoch EÚ alebo v právnych predpisoch členských štátov, ktorým podlieha prevádzkovateľ. Úlohy vykonávané vo verejnom záujme tretej krajiny alebo v rámci výkonu úradného orgánu udelené podľa cudzieho práva nepatria do rozsahu pôsobnosti tohto ustanovenia podľa staršej smernice 95/46 a tento prístup pokračuje v GDPR.

Táto analógia tohto ustanovenia podľa staršej smernice sa používala na pokrytie dvoch rôznych situácií:

(i) ak samotný prevádzkovateľ reprezentuje verejný záujem alebo plní úlohu verejného záujmu (ale nie je nevyhnutne povinný spracovávať údaje) a spracovanie je nevyhnutné na výkon tohto orgánu alebo na vykonávanie tejto úlohy, alebo

(ii) ak prevádzkovateľ nedisponuje úradnou mocou, ale je požiadaný treťou stranou, ktorá má takúto právomoc zverejniť údaje data[ix].

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

GDPR odstránila druhé kritérium, t. j. situácie, v ktorých je výkon verejnej moci udelený strane, ktorej údaje sú zverejnené a nie sú viac **relevantné** ako dôvod na spracovanie údajov[x]. Inak povedané, okolnosti, za ktorých sa kontrolór môže opierať o tento právny základ, sú užšie ako predtým.

Úradný orgán alebo verejná úloha by mali byť zvyčajne pripísané právnym zákonom alebo iným právnym predpisom. WP29 výslovne uznal, že po GDPR je potrebné tento právny základ vykladať tak, aby verejným orgánom poskytol určitý stupeň flexibility na zabezpečenie ich správneho riadenia a fungovania. Takéto činnosti by preto nemali patriť do pôsobnosti tohto právneho rámca a spracovanie osobných údajov by mohlo byť založené na legitímnom záujme.

V neposlednom rade treba poznamenať, že subjekty údajov majú právo vzniesť námietku voči spracovaniu založenému na tomto právnom základe. Prevádzkovateľ je povinný preukázať, že má presvedčivé legitímne dôvody na spracovanie osobných údajov[xi].

2.5.2. Uplatniteľnosť v kontexte činnosti Miestnych orgánov

Medzi zákonnou povinnosťou podľa čl. 6, odst. 1, bod "c" GDPR, by úloha vykonávaná vo verejnom záujme / výkon úradnej moci je jedným z najdôležitejších právnych dôvodov pre činnosť orgánov činných v trestnom konaní. Príklady WP29 na uplatnenie tohto dôvodu zahŕňajú:

- daňový orgán, ktorý zhromažďuje a spracúva daňové priznanie jednotlivca s cieľom stanoviť a overiť výšku dane, ktorá sa má zaplatiť - analogicky by sa tento dôvod mohol uplatňovať aj na miestne orgány, ktoré spravujú miestne dane;
- orgán miestnej samosprávy (napríklad obecný úrad) poverený úlohou prevádzkovať knižnicu, školu alebo miestnu plaváreň.

2.6. Právne záujmy

2.6.1. Význam a právne požiadavky

Právny dôvod "legitímne záujmy" zahŕňa dva prvky:

(i) Legitímny záujem správcu údajov / tretích strán

a. Pojem "záujem" definuje WP29 ako širší podiel, ktorý môže mať prevádzkovateľ pri spracovaní, alebo výhodu, ktorú riadiaci organ odvodí - alebo že spoločnosť môže odvodiť - zo spracovania. Záujem môže byť prínosom pre spoločnosť vo všeobecnosti, ale môže byť prínosom aj pre príslušného správcu údajov / tretiu stranu;

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

b. Pojem "legitímnosť" je neodmysliteľne spojený s dodržiavaním zákona - zákonom o ochrane údajov, ako aj zákonmi platnými pre príslušnú činnosť prevádzkovateľa. Inými slovami, akékoľvek nezákonné ciele sledované prevádzkovateľom / treťou stranou by diskvalifikovali uplatniteľnosť tohto právneho dôvodu. WP29 urobila **nevyčerpávajúci** zoznam najbežnejších scenárov, v ktorých by sa mohol uplatniť oprávnený záujem podľa staršej smernice 95/46. Oblasti sa líšia z hľadiska reklamy alebo pozornosti (napr. priamy marketing, reklama alebo nevyžiadané nekomerčné správy vrátane politických kampaní alebo charitatívneho fundraisingu) na činnosti spoločenskej povahy (napr. schémy oznamovania, uplatňovanie práva na slobodu prejavu alebo informácie alebo predchádzanie podvodom, zneužívaniu služieb alebo praniu špinavých peňazí).

(ii) Legitímny záujem by mal prevažovať nad záujmami, základnými právami a slobodami a dotknutou osobou = skúška vyváženosti by sa mala uplatňovať od prípadu k prípadu. Táto požiadavka je vo svojej podstate spojená so zásadou proporcionality. Hoci správca údajov / tretia strana môže mať legitímny záujem na spracovaní, mohlo by sa javiť ako neprimerané (napr. príslušné spracovanie by mohlo mať nepriaznivý vplyv, príliš veľký rozsah, bez primeraných obmedzení a záruk atď.) A v takomto prípade spracovanie by nebolo opodstatnené ako zákonné. WP29 uviedla, že medzi faktory potrebné na vykonanie testu vyváženosti sú:

a. posúdenie oprávneného záujmu prevádzkovateľa;

b. vplyv na dotknuté osoby;

c. predbežný zostatok a

d. dodatočné bezpečnostné opatrenia, ktoré používa prevádzkovateľ, aby sa zabránilo neprimeranému vplyvu na dotknuté osoby[xii].

2.6.2. Uplatniteľnosť v kontexte činnosti Miestnych orgánov

GDPR výrazne obmedzuje uplatniteľnosť oprávneného záujmového prostredia v kontexte činností verejných orgánov. V GDPR sa výslovne ustanovuje, že tento právny základ sa nevzťahuje na spracovanie vykonávané orgánmi verejnej správy pri výkone ich úloh. Dôvodom tohto ustanovenia je, že verejné orgány by mali byť zo zákona oprávnené vykonávať svoje úlohy.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

Preto je vhodné, aby sa MO, ktoré sa opierajú o legitímny záujem na plnenie svojich úloh, opätovne posúdili, aký iný právny základ na spracovanie osobných údajov by mohli uplatňovať (napríklad úloha vo verejnom záujme / verejnej moci).

Legitímny záujem by však ešte mohli uplatňovať miestne orgány ako platný právny základ pre ich vnútorné procesy - napr. vo svojich aktivitách v oblasti ľudských zdrojov.

3. Záver a Praktické rady

Schopnosť určiť, ktorý právny základ sa bude uplatňovať pre tú ktorú spracovateľskú činnosť, ktoré je nevyhnutná pre každého správcu údajov, aby bola zabezpečená zákonnosť spracovania. Okrem toho informácie, ktoré sa týkajú právneho základu, a na ktorý účel spracovania je jedným z kľúčových prvkov zásady transparentnosti, pretože je výslovne zahrnuté medzi informácie, ktoré musí prevádzkovateľ poskytnúť každej dotknutej osobe (článok 13 a článok 3 ods. 14 GDPR). Preto by verejní aj súkromní prevádzkovatelia údajov mali byť oboznámení s každým z právnych dôvodov uvedených v čl. 6 GDPR. Nariadenie neustanovuje nové právne dôvody, ale skôr upravuje požiadavky a podmienky uplatniteľnosti pre niektoré existujúce právne predpisy (napríklad súhlas, oprávnené záujmy). V každom prípade je schopnosť identifikovať správny právny základ ako prvý krok k zabezpečeniu dodržiavania pravidiel GDPR v rámci organizácie. V doktríne sa uvádza, že obozretný správca údajov by mal podniknúť potrebné kroky, aby zaručil, že v prípadoch, keď orgány dohľadu vyžadujú dôkazy, prevádzkovateľ by mal byť schopný poukázať na to, o aké kritériá sa opiera o spracovanie a správne oznamovanie subjekty údajov[xiii].

4. Externé zdroje a webové stránky

Knihy

- **Voigt, P., von dem Bussche, A.**, The EU General Data Protection Regulation (GDPR) – A Practical Guide, Springer International Publishing (2017);
- **Boardman, R., Mullock, J., Mole, A.** Bird & Bird Guide to General Data Protection Regulation (2016);
- **EU** General Data Protection Regulation (GDPR). An Implementation and Compliance Guide, IT Governance Publishing, Cambridgeshire (2016);
- **European** Data Protection. Law and Practice, Executive Editor: Edurado Ustaran, CIPP/E, Partner, Hogan Lovells, IAPP (2018);

Dokumenty článku 29

- WP29, Guidelines on Consent under Regulation 2016/679, WP 259;

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

- WP29, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, WP 217;

Web Links

- http://europa.eu/rapid/press-release_IP-18-386_en.htm
- https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en
- https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/grounds-processing/when-can-personal-data-be-processed_en
- https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/grounds-processing/what-does-grounds-legitimate-interest-mean_en
- https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/grounds-processing/when-consent-valid_en
- https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/grounds-processing/does-consent-given-25-may-2018-continue-be-valid-once-gdpr-starts-apply-25-may-2018_en
- https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/grounds-processing/what-if-somebody-withdraws-their-consent_en
- https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/grounds-processing/what-if-somebody-withdraws-their-consent_en

5. REFERENCIE

[i] WP29, Guidelines on Consent under Regulation 2016/679, WP 259, p. 13.
[ii] The example is given in WP29, Guidelines on Consent under Regulation 2016/679, WP 259, p. 7.
[iii] European Data Protection. Law and Practice, Executive Editor: Edurado Ustaran, CIPP/E, Partner, Hogan Lovells, IAPP (2018), p. 118
[iv] WP29 Opinion 06/2014 on the notion of legitimate interests of the data controllerunder Article 7 of Directive 95/46/EC, WP 217, p. 16.
[v] Boardman, R., Mullock, J., Mole, A.Bird & Bird Guide to General Data Protection Regulation (2016), p. 10.
[vi] Ibid, p. 19.
[vii] Ibid, p. 20.
[viii] Ibid, p. 19.
[ix] Ibid, p. 21.
[x] European Data Protection. Law and Practice, Executive Editor: Edurado Ustaran, CIPP/E, Partner, Hogan Lovells, IAPP (2018), p. 119.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

[xi] European Data Protection. Law and Practice, Executive Editor: Edurado Ustaran, CIPP/E, Partner, Hogan Lovells, IAPP (2018), p. 119.
[xii] Ibid, p. 33.
[xiii] European Data Protection. Law and Practice, Executive Editor: Edurado Ustaran, CIPP/E, Partner, Hogan Lovells, IAPP (2018), p. 122.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

ProLegis

Spracovanie osobitných kategórií osobných údajov

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

ProLegis

Contents

1. PRÁVNY RÁMEC 4
   1.1. Charta základných práv EU 4
   1.2. GDPR 4
2. ŠPECIÁLNE KATEGÓRIE OSOBNÝCH ÚDAJOV V ZMYSLE GDPR 10
   2.1. Logika pri vymedzovaní určitých kategórii osobných údajov 10
   2.2. Typy špeciálnych kategórii osobných údajov 10
   2.3. Osobné údaje týkajúce sa trestných rozsudkov a trestných činov 12
3. PRÁVNE DÔVODY PRE SPRACOVANIE OSOBITNÝCH KATEGÓRIÍ OSOBNÝCH ÚDAJOV 13
   3.1. Výslovný súhlas 13
   3.2. Povinnosti / osobitné práva v oblasti práva zamestnanosti, sociálneho zabezpečenia a sociálnej ochrany 14
   3.3. Životne dôležitý záujem dotknutej osoby alebo inej fyzickej osoby 15
   3.4. Spracovanie neziskového subjektu/organizácie s politickým, filozofickým, náboženským alebo odborovým cieľom 15
   3.5. Dáta sú verejne zverejňované subjektom údajov 15
   3.6. Zriadenie, výkon alebo obhajoba súdnych pohľadávok / súdov konajúcich v ich súdnej funkcii 16
   3.7. Základný verejný záujem na základe právnych predpisov EÚ alebo členských štátov 16
   3.8. Preventívne alebo pracovné lekárstvo, hodnotenie pracovnej schopnosti zamestnanca, lekárska diagnostika, poskytovanie zdravotnej alebo sociálnej starostlivosti alebo liečby 17
   3.9. Verejný záujem v oblasti verejného zdravia 17
   3.10. Spracovanie na účely archivácie vo verejnom záujme, vedecké alebo historicko-výskumné účely alebo štatistické účely 18
   3.11. Ďalšie podmienky vpráve členských štátov 18

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

4. ZÁVER A PRAKTICKÉ RADY 18
5. EXTERNÉ ZDROJE A WEBOWÉ LINKY 19
Knihy 19
Documents of the Article 29 Working Party 19
Web Links 19
6. REFERENCIE 19

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

1. PRÁVNY RÁMEC

1.1. Charta základných práv EU

Článok 8

Ochrana osobných údajov

1. Každý má právo na ochranu osobných údajov, ktoré sa ho týkajú.

2. Tieto údaje musia byť riadne spracované na určené účely **na základe súhlasu dotknutej osoby alebo na inom oprávnenom základe ustanovenom zákonom.** Každý má právo na prístup k zhromaždeným údajom, ktoré sa ho týkajú, a právo na ich opravu

3. Dodržiavanie týchto pravidiel podlieha kontrole nezávislého orgánu

1.2. GDPR

Recitál (51)

Osobné údaje, ktoré sú svojou povahou obzvlášť citlivé v súvislosti so základnými právami a slobodami, si zasluhujú osobitnú ochranu, keďže z kontextu ich spracúvania by mohli pre základné práva a slobody vyplývať významné riziká. Uvedené osobné údaje by mali zahŕňať osobné údaje, ktoré odhaľujú rasový alebo etnický pôvod, pričom použitie výrazu „rasový pôvod“ v tomto nariadení neznamená, že Únia akceptuje teórie, ktoré sa usilujú stanoviť existenciu oddelených ľudských rás. Spracúvanie fotografií by sa nemalo systematicky považovať za spracúvanie osobitných kategórií osobných údajov, pretože vymedzenie pojmu biometrické údaje sa na ne bude vzťahovať len v prípadoch, keď sa spracúvajú osobitnými technickými prostriedkami, ktoré umožňujú alebo potvrdzujú jedinečnú identifikáciu fyzickej osoby. Takéto osobné údaje by sa nemali spracúvať, pokiaľ spracúvanie nie je povolené v osobitných prípadoch stanovených v tomto nariadení, pričom sa zohľadní, že právo členských štátov môže stanoviť osobitné ustanovenia o ochrane údajov, ktorými prispôsobia uplatňovanie pravidiel tohto nariadenia na účely splnenia zákonnej povinnosti alebo úlohy realizovanej vo verejnom záujme či pri výkone verejnej moci zverenej prevádzkovateľovi. Okrem osobitných požiadaviek na takéto spracúvanie by sa mali uplatňovať všeobecné zásady a iné pravidlá uvedené v tomto nariadení, najmä pokiaľ ide o podmienky pre zákonné spracúvanie. Výnimky zo všeobecného zákazu spracúvania týchto osobitných kategórií

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

osobných údajov by sa mali výslovne uviesť okrem iného vtedy, ak dotknutá osoba poskytla svoj výslovný súhlas alebo v súvislosti s osobitnými potrebami, najmä ak spracúvanie vykonávajú v rámci legitímnych činností určité združenia alebo nadácie, ktorých účelom je umožniť výkon základných slobôd.

Recitál (52)

Výnimka zo zákazu spracúvania osobitných kategórií osobných údajov by sa taktiež mala povoliť, ak je to stanovené v práve Únie alebo v práve členského štátu, a za splnenia vhodných záruk, aby boli chránené osobné údaje a iné základné práva, ak to odôvodňuje verejný záujem, najmäspracúvanie osobných údajovv oblasti pracovného práva, práva sociálnej ochrany vrátane dôchodkového zabezpečenia, a na účely zdravotnej bezpečnosti, monitorovania a varovania, prevencie alebo kontroly prenosných chorôb a iných závažných hrozieb pre zdravie. Takáto výnimka sa môže vykonať na zdravotné účely vrátane verejného zdravia a riadenia služieb zdravotnej starostlivosti, najmä s cieľom zabezpečiť kvalitu a nákladovú efektívnosť postupov používaných na uspokojovanie nárokov na plnenie a služby v systéme zdravotného poistenia, alebo na účely archivácie vo verejnom záujme, na účely vedeckého alebo historického výskumu alebo na štatistické účely. Výnimka by sa mala povoliť aj na spracúvanie takýchto osobných údajov, ak je to potrebné na preukazovanie, uplatňovanie alebo obhajovanie právnych nárokov, a to bez ohľadu na to, či ide súdne alebo správne konanie alebo mimosúdne konanie.

Recitál (53)

Osobitné kategórie osobných údajov, ktoré si zasluhujú vyššiu ochranu, by sa mali spracúvať len na zdravotné účely, ak je to potrebné na dosiahnutie týchto účelov v prospech fyzických osôb a spoločnosti ako celku, najmä v súvislosti s riadením služieb a systémov zdravotnej alebo sociálnej starostlivosti vrátane spracúvania takýchto údajov manažmentom a ústrednými národnými zdravotníckymi orgánmi na účely kontroly kvality, informácií potrebných pre riadenie a všeobecného vnútroštátneho a miestneho dohľadu nad systémom zdravotnej alebo sociálnej starostlivosti, a zabezpečenia kontinuity zdravotnej alebo sociálnej starostlivosti a cezhraničnej zdravotnej starostlivosti alebo zdravotnej bezpečnosti, monitorovania a varovných účelov, alebo na účely archivácie vo verejnom záujme, na účely vedeckého alebo historického výskumu alebo na štatistické účely na základe práva Únie alebo práva členského štátu, ktoré musí spĺňať cieľ verejného záujmu, ako aj na štúdie uskutočňované vo verejnom záujme v oblasti verejného zdravia. Týmto nariadením by sa preto mali stanoviť harmonizované

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

podmienky pre spracúvanie osobitných kategórií osobných údajov týkajúcich sa zdravia v súvislosti s osobitnými potrebami, najmä ak spracúvanie takýchto údajov vykonávajú na určité zdravotné účely osoby, na ktoré sa vzťahuje zákonná povinnosť zachovania profesijného tajomstva. V práve Únie alebo v práve členského štátu by sa mali stanoviť osobitné a vhodné opatrenia na ochranu základných práv a osobných údajov fyzických osôb. Členským štátom by sa malo umožniť zachovať alebo zaviesť ďalšie podmienky vrátane obmedzení týkajúce sa spracúvania genetických údajov, biometrických údajov alebo údajov týkajúcich sa zdravia. To by však nemalo brániť voľnému toku osobných údajov v rámci Únie, keď sa tieto podmienky vzťahujú na cezhraničné spracúvanie takýchto údajov.

Recitál (54)

Spracúvanie osobitných kategórií osobných údajov bez súhlasu dotknutej osoby môže byť potrebné z dôvodov verejného záujmu v oblasti verejného zdravia. Takéto spracúvanie by malo podliehať vhodným a konkrétnym opatreniam na ochranu práv a slobôd fyzických osôb. V tejto súvislosti by sa malo „verejné zdravie“ vykladať v zmysle nariadenia Európskeho parlamentu a Rady (ES) č. 1338/2008 (1), teda malo by zahŕňať všetky prvky týkajúce sa zdravia, a to zdravotný stav vrátane chorobnosti a zdravotného postihnutia, faktory ovplyvňujúce tento zdravotný stav, potreby zdravotnej starostlivosti, zdroje pridelené na zdravotnú starostlivosť, poskytovanie

zdravotnej starostlivosti a jej všeobecnú dostupnosť, ako aj výdavky na zdravotnú starostlivosť a jej financovanie, a príčiny smrti. Takéto spracúvanie údajov týkajúcich sa zdravia z dôvodov verejného záujmu by nemalo viesť k spracúvaniu osobných údajov na iné účely tretími stranami, napríklad zamestnávateľmi či poisťovňami a bankami.

Recitál (55)

Okrem toho sa spracúvanie osobných údajov oficiálnymi orgánmi na účel dosiahnutia cieľov oficiálne uznaných náboženských združení, pričom ide o ciele stanovené ústavným právom alebo medzinárodným právom verejným, vykonáva vo verejnom záujme.

Recitál (56)

Ak si počas volebných aktivít fungovanie demokratického systému v niektorom členskom štáte vyžaduje, aby politické strany zhromažďovali osobné údaje o politických názoroch

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

ľudí, môže byť spracúvanie takýchto údajov povolené z dôvodov verejného záujmu, a to za predpokladu, že sú

Článok 4

Vymedzenie pojmov

Na účely tohto nariadenia:

[…]

(13) ***„genetické údaje“*** *sú osobné údaje týkajúce sa zdedených alebo nadobudnutých genetických charakteristických znakov fyzickej osoby, ktoré poskytujú jedinečné informácie o fyziológii alebo zdraví tejto fyzickej osoby a ktoré vyplývajú najmä z analýzy biologickej vzorky danej fyzickej osoby;*

*(14) ‘**biometrické údaje“** sú osobné údaje, ktoré sú výsledkom osobitného technického spracúvania, ktoré sa týka fyzických, fyziologických alebo behaviorálnych charakteristických znakov fyzickej osoby a ktoré umožňujú alebo potvrdzujú jedinečnú identifikáciu tejto fyzickej osoby, ako napríklad vyobrazenia tváre alebo daktyloskopické údaje;*

*(15) **„údaje týkajúce sa zdravia**“ sú osobné údaje týkajúce sa fyzického alebo duševného zdravia fyzickej osoby, vrátane údajov o poskytovaní služieb zdravotnej starostlivosti, ktorými sa odhaľujú informácie o jej zdravotnom stave;*

Článok 9

Spracúvanie osobitných kategórií osobných údajov

1. Zakazuje sa spracúvanie osobných údajov, ktoré odhaľujú rasový alebo etnický pôvod, politické názory, náboženské alebo filozofické presvedčenie alebo členstvo v odborových organizáciách, a spracúvanie genetických údajov, biometrických údajov na individuálnu identifikáciu fyzickej osoby, údajov týkajúcich sa zdravia alebo údajov týkajúcich sa sexuálneho života alebo sexuálnej orientácie fyzickej osoby.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

2. **Odsek 1 na neuplatňuje** ak platí niektorá z týchto podmienok:

(a) dotknutá osoba vyjadrila výslovný súhlas so spracúvaním týchto osobných údajov na jeden alebo viacero určených účelov, s výnimkou prípadov, keď sa v práve Únie alebo v práve členského štátu stanovuje, že zákaz uvedený v odseku 1 nemôže dotknutá osoba zrušiť;

(b) spracúvanie je nevyhnutné na účely plnenia povinností a výkonu osobitných práv prevádzkovateľa alebo dotknutej osoby v oblasti pracovného práva a práva sociálneho zabezpečenia a sociálnej ochrany, pokiaľ je to povolené právom Únie alebo právom členského štátu alebo kolektívnou zmluvou podľa práva členského štátu poskytujúcimi primerané záruky ochrany základných práv a záujmov dotknutej osoby;

(c) spracúvanie je nevyhnutné na ochranu životne dôležitých záujmov dotknutej osoby alebo inej fyzickej osoby v prípade, že dotknutá osoba nie je fyzicky alebo právne spôsobilá vyjadriť svoj súhlas;

(d) spracúvanie vykonáva v rámci svojej zákonnej činnosti s primeranými zárukami nadácia, združenie alebo akýkoľvek iný neziskový subjekt s politickým, filozofickým, náboženským alebo odborárskym zameraním a pod podmienkou, že spracúvanie sa týka výlučne členov alebo bývalých členov subjektu alebo osôb, ktoré majú pravidelný kontakt s ním v súvislosti s jeho cieľmi, a že bez súhlasu dotknutej osoby sa osobné údaje neposkytnú mimo tohto subjektu;

(e) spracúvanie sa týka osobných údajov, ktoré dotknutá osoba preukázateľne zverejnila;

(f) spracúvanie je nevyhnutné na preukazovanie, uplatňovanie alebo obhajovanie právnych nárokov, alebo kedykoľvek, keď súdy vykonávajú svoju súdnu právomoc;

(g) spracovanie je nevyhnutné z dôvodov významného verejného záujmu na základe práva Únie alebo členského štátu, ktorý je primeraný sledovanému cieľu, rešpektuje podstatu práva na ochranu údajov a ustanovuje vhodné a osobitné opatrenia na ochranu základných práv a záujmom dotknutej osoby;

(h) spracovanie je nevyhnutné na účely preventívnej alebo pracovnej medicíny, na posúdenie pracovnej schopnosti zamestnanca, lekárskej diagnostiky, poskytovania zdravotnej alebo sociálnej starostlivosti alebo liečby alebo na riadenie systémov a služieb zdravotnej starostlivosti alebo sociálnej starostlivosti na základe práva Únie alebo členského štátu alebo na základe zmluvy s odborníkom v oblasti zdravotníctva s podmienkami a zárukami uvedenými v odseku 3;

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

(i) spracovanie je nevyhnutné z dôvodov verejného záujmu v oblasti verejného zdravia, ako je ochrana pred vážnymi cezhraničnými ohrozeniami zdravia alebo zabezpečenie vysokých noriem kvality a bezpečnosti zdravotnej starostlivosti a liekov alebo zdravotníckych pomôcok na základe právnych predpisov Únie alebo právne predpisy členského štátu, ktoré stanovujú vhodné a osobitné opatrenia na ochranu práv a slobôd dotknutej osoby, najmä služobné tajomstvo;

(j) spracovanie je potrebné na účely archivácie vo verejnom záujme, na účely vedeckého alebo historického výskumu alebo na štatistické účely v súlade s článkom 89 ods. 1 na základe právnych predpisov Únie alebo členských štátov, ktoré sú primerané sledovanému cieľu, rešpektujú podstatu práva na ochranu údajov a zabezpečiť vhodné a osobitné opatrenia na ochranu základných práv a záujmov dotknutej osoby.

3. Osobné údaje uvedené v odseku 1 sa môžu spracúvať na účely uvedené v odseku 2 písm. h), ak tieto údaje spracúva odborník, alebo ak sa spracúvajú v rámci zodpovednosti odborníka, ktorý podlieha povinnosti zachovávať profesijné tajomstvo podľa práva Únie alebo práva členského štátu alebo podľa pravidiel, ktoré stanovili príslušné vnútroštátne orgány, alebo ak údaje spracúva iná osoba, ktorá tiež podlieha povinnosti mlčanlivosti podľa práva Únie alebo práva členského štátu alebo pravidiel, ktoré stanovili príslušné vnútroštátne orgány.

4. Členské štáty môžu zachovať alebo zaviesť ďalšie podmienky vrátane obmedzení týkajúce sa spracúvania genetických údajov, biometrických údajov alebo údajov týkajúcich sa zdravia.

Článok 10

Spracúvanie osobných údajov týkajúcich sa uznania viny za trestné činy a priestupky

Spracúvanie osobných údajov týkajúcich sa uznania viny za trestné činy a priestupky alebo súvisiacich bezpečnostných opatrení založených na článku 6 ods. 1 sa vykonáva **len pod kontrolou orgánu verejnej moci, alebo ak je spracúvanie povolené právom Únie alebo právom členského štátu** poskytujúcim primerané záruky ochrany práv a slobôd dotknutých osôb. Každý komplexný register uznania viny za trestné činy sa vedie iba pod kontrolou orgánu verejnej moci.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

2. ŠPECIÁLNE KATEGÓRIE OSOBNÝCH ÚDAJOV V ZMYSLE GDPR

2.1. Logika pri vymedzovaní určitých kategórii osobných údajov

Dokonca aj v priebehu prípravy prvého právneho aktu EÚ venovaného ochrane osobných údajov - smernici 95/46 - Európska komisia zdôraznila, že spracovanie určitých kategórií osobných údajov by mohlo znamenať vyššie riziko pre základné práva a slobody európskych občanov. Preto bol stanovený všeobecný zákaz spracovania takýchto "riskantných" kategórií osobných údajov. Boli nazývané "špeciálne kategórie osobných údajov", ale v praxi sa nazývali aj "citlivé údaje" kvôli ich citlivej povahe pre súkromnú sféru jednotlivca. Takéto údaje by sa mohli spracúvať len za výnimočných okolností, ktoré sú taxatívne vymenované v právnych predpisoch členských štátov o ochrane údajov.

GDPR pokračuje v tomto prístupe, ale rozširuje rozsah osobitných kategórií osobných údajov a stanovuje niektoré nové výnimky (právne dôvody), ktoré oprávňujú kontrolórov na spracovávanie takýchto údajov.

Treba spomenúť, že rôzne typy údajov majú odlišný vplyv jednotlivcov. Ktoré údaje sú definované ako citlivé, je založené na objektívnom, a nie na subjektívnom princípe. Inými slovami, niekto môže mať pocit, že údaje týkajúce sa ich finančného stavu, histórie disciplinárnych sankcií alebo jedinečného identifikačného čísla / čísla sociálneho poistenia sú citlivé. Napriek tomu, ak takéto údaje európsky zákonodarca neuzná ako citlivý, nespadajú pod osobitný režim spracovania takýchto údajov bez ohľadu na ich citlivú povahu zo subjektívnych hľadísk.

V doktríne sa uvádza, že voľba, ktoré kategórie osobných údajov sa majú definovať ako osobitné, bola podstatne ovplyvnená antidiskriminačnými zákonmi, čo vysvetľuje, prečo sú údaje, ako sú čísla sociálneho zabezpečenia a údaje o kreditných kartách (ktoré by v prípade zneužitia mohli spôsobiť vážnu ujmu jednotlivcom) nie sú definované ako citlivé.

2.2. Typy špeciálnych kategórii osobných údajov

Podľa čl. 9, odsek 1 GDPR, nasledujúce kategórie osobných údajov sú osobitné kategórie (citlivé údaje):

- **Osobné údaje, ktoré odhaľujú rasový alebo etnický pôvod** = tieto kategórie osobných údajov sú definované ako citlivé, pretože predstavujú vysoké riziko

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

diskriminácie. V právnej doktríne sa uvádzajú nasledovné príklady, ktoré by mohli spadať do tejto kategórie: meno a priezvisko osoby, miesto jeho narodenia, rodný jazyk alebo mená jeho rodičov, ktoré by mohli pri kombinácii umožňovať závery týkajúce sa jeho pôvodi;

- **Politické názory** = tieto údaje si zaslúžia osobitnú ochranu, pretože súvisia so zárukou, že občania vytvárajú názory na politiku a nakoniec sa zúčastňujú (aktívne ako politici a / alebo pasívne ako voliči a členovia občianskej spoločnosti) v politickom živote krajiny. Príklady takýchto údajov zahŕňajú informácie o členstve politických strán, informácie týkajúce sa zapojenia sa do akýchkoľvek petícií, účasti na demonštráciách, politických stretnutiach alebo podobných podujatiach, informácií o podpore určitej politickej myšlienky alebo jej odmietnutí.
- **Politické názory alebo filozofické svetonázory** = tieto údaje si zasluhujú osobitnú ochranu, pretože sú zárukou, že občania budú tvoriť politické názory a nakoniec sa zúčastnia (aktívne ako politici a / alebo pasívne ako voliči a členovia občianskej spoločnosti) v politickom živote krajiny. Príklady takýchto údajov zahŕňajú informácie o členstve politických strán, informácie týkajúce sa zapájania sa do akýchkoľvek petícií, účasti na demonštráciách, politických stretnutiach alebo podobných podujatiach, informácií o podpore určitej politickej myšlienky alebo jej odmietnutí
- **Členstvo v odboroch** = informácie týkajúce sa takýchto členstva sú citlivé, pretože vytvárajú riziko diskriminačného zaobchádzania v oblasti pracovného práva. Európski občania majú slobodu kolektívneho vyjednávania a konania, a preto by nemali byť nerovnako zaobchádzaní na základe ich odborovej príslušnostiii;
- **Genetické údaje** = nová kategória zavedená GDPR, definovaná ako citlivé údaje. GDPR ju definuje ako "údaje týkajúce sa zdedených alebo získaných genetických vlastností fyzickej osoby, ktoré poskytujú jedinečné informácie o fyziológii alebo zdraví tejto fyzickej osoby a ktoré vyplývajú najmä z analýzy biologickej vzorky od fyzickej osoby v otázke'. Niektoré členské štáty už udelili štatút citlivosti tohto druhu údajov, ale GDPR ho prvýkrát zaviedol na úrovni EÚ. Genetické údaje by mali byť chránené, pretože takéto údaje sa týkajú nielen príslušného subjektu údajov, ale môžu tiež ovplyvniť nedefinovaný okruh osôb, ktoré sú súčasťou rodokmeňa subjektu (vrátane údajov o úmrtiach, údajoch detí atď.). Navyše podrobná analýza takýchto údajov by mohla odhaliť ďalšie typy citlivých informácií, ako sú psychologické alebo zdravotné údaje (napríklad predispozícia k chorobám, zraniteľnosť atď.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

- **Biometrické údaje na účely jednoznačnej identifikácie fyzickej** osoby = takéto typy údajov si zaslúžia ochranu, pretože umožňujú kontrolórom jednoznačne identifikovať danú fyzickú osobu na základe jej fyzických alebo behaviorálnych vlastností: odtlačky prstov, rozpoznanie tváre, dúhovka, sietnica, vaskulárne modely, DNA, reč, podpis, klávesová interakcia atď.). Keďže spracovanie takýchto typov údajov sa stáva čoraz bežnejším pri zavádzaní rôznych technologických rozhodnutí (napr. Systémy na kontrolu prístupu do priestorov, systémy na identifikáciu na vzdialených zariadeniach, ako sú mobilné telefóny, tablety atď.), Takéto spracovanie by malo byť viac obmedzujúce a kontrolované a tieto faktory odôvodňujú zahrnutie týchto údajov do zoznamu "citlivých" údajov v rámci GDPR. Na rozdiel od postupov zavedených v niektorých členských štátoch nebude spracovanie fotografií automaticky považované za citlivé spracovanie. Fotografie budú považované za citlivé údaje len vtedy, ak umožnia jedinečnú identifikáciu alebo autentifikáciu osoby ako biometrickej (napríklad v elektronickom pase alebo inom type dokladu totožnosti)iii;
- **Údaje týkajúce sa zdravia alebo údajov týkajúcich sa sexuálneho života alebo sexuálnej orientácie fyzickej osoby** = takéto údaje sú veľmi citlivé, pretože zasahujú do najintímnejších aspektov života jednotlivca. Okrem toho informácie týkajúce sa sexuálneho života a sexuálnej orientácie predstavujú riziko diskriminácie, manipulácie atď. V teórii sa uvádza, že tieto údaje zahŕňajú aj presnú identitu partnera(ov/iek).

2.3. Osobné údaje týkajúce sa trestných rozsudkov a trestných činov

Osobné údaje týkajúce sa trestných rozsudkov a trestných činov, alebo súvisiacich bezpečnostných opatrení nie sú vyhlásené za osobitnú kategóriu osobných údajov. Napriek tomu právne predpisy niektorých členských štátov ich považujú za citlivé. Napriek tomu však takéto informácie zahŕňajú aj riziko nerovnakého zaobchádzania (napríklad v oblasti zamestnania), a preto sa na tieto údaje vzťahujú aj osobitné pravidlá spracovania. V súvislosti so starou smernicou 95/46 v súvislosti s trestnými rozsudkami a údajmi o trestných činoch GDPR nezavádza významné zmeny a doplnenia. Zároveň by vzhľadom na skutočnosť, že pravidlá smernice boli v členskom štáte transponované rôznymi spôsobmi, by GDPR zaviedol všeobecnejší prístup na úrovni EÚ k takýmto údajom. Podľa znenia článku 4 ods. 10 GDPR, tieto údaje by mohli byť spracované na základe jedného z dôvodov článku. 6 za predpokladu, že je splnená jedna z dvoch **alternatívnych** dodatočných podmienok:

(i) Spracovanie by malo byť pod kontrolou úradnej inštitúcie, alebo

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

(ii) Spracovanie je povolené právnymi predpismi EU / členských štátov, ktoré zabezpečujú primerané záruky práv a slobôd dotknutých osôb.

Existuje tak povediac neistota v súvislosti s týmto ustanovením, pretože nie je jasné, ako sa tieto dve dodatočné požiadavky, ktoré sa na ňu vzťahujú, uplatňujú spolu s článkom 6. Konzervatívny výklad spočíva v tom, že súkromné alebo obchodné subjekty nemôžu spracovávať tieto údaje, inými slovami "v nariadení nie je priestor na súkromné alebo obchodné spracovanie týchto údajov". Druhý výklad spočíva v tom, že takýto typ údajov by mohol byť spracovaný na základe všetkých možných právnych dôvodov za predpokladu, že sú splnené dodatočné podmienky (pod kontrolou úradnej inštitúcie, alebo v prípade ak to umožňuje uplatniteľné právo). V doktríne sa uvádza, že toto ustanovenie by pravdepodobne viedlo k pokračovaniu národných rozdielov. Hoci miestne orgány budú pôsobiť ako orgány verejnej moci a teoreticky by mohli odôvodniť prvú dodatočnú požiadavku na spracovanie (pod kontrolou úradných orgánov), bolo by vhodné, aby sa starostlivo preskúmali miestne predpisy, aby sa tieto typy údajov mohli spracúvať (najmä v súvislosti s aktivitami v oblasti ľudských zdrojov a zhromažďovaním záznamov o trestnom registri, pretože príslušný MO koná ako zamestnávateľ v tomto kontexte, a nie ako držiteľ verejnej moci, a uplatniteľnosť prvej dodatočnej podmienky je sporná).

3. PRÁVNE DÔVODY PRE SPRACOVANIE OSOBITNÝCH KATEGÓRIÍ OSOBNÝCH ÚDAJOV

Všeobecný zákaz spracovania osobitných kategórií osobných údajov sa neuplatňuje za predpokladu, že je splnená jedna z nasledujúcich **alternatívnych** podmienok:

3.1. Výslovný súhlas

Požiadavky, ktoré musia byť splnené v rámci GDPR, aby mali platný súhlas (slobodne udelený, špecifický, informovaný, jednoznačný), sa v každom prípade vzťahuje na spracovanie osobných údajov osobitných kategórií. Pojem "explicitný" nie je definovaný v GDPR. Pracovná skupina zriadená podľa článku 29 (WP29) uvádza, že je potrebný výslovný súhlas v situáciách, kedy by sa mohlo objaviť vážne riziko ochrany údajov a je zabezpečená primeraná vysoká úroveň individuálnej kontroly osobných údajoviv.

Pojem "explicitné" sa vzťahuje na spôsob vyjadrenia súhlasu dotknutej osoby - subjekt údajov musí poskytnúť vyhlásenie o výslovnom súhlase. Jedným zo spôsobov, ako udeliť súhlas v., je výslovne potvrdiť v písomnom vyhlásení.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

V on-line kontexte by sa rôzne riešenia dali uplatniť vyplnením elektronickej formy, zaslaním e-mailu, odoslaním naskenovaného dokumentu s podpisom dotknutej osoby, alebo použitím elektronického podpisu. Akékoľvek iné prostriedky, ktoré by umožnili kontrolórovi preukázať primeraný spôsob, akým má byť súhlas udelený.

Vzhľadom na nerovnováhu právomocí medzi dotknutými osobami a verejnými orgánmi sa neodporúča, aby sa miestne orgány spoliehali predovšetkým na výslovný súhlas so spracovaním osobitných kategórií osobných údajov (vrátane vzťahov s občanmi a zamestnancami).

3.2. Povinnosti / osobitné práva v oblasti práva zamestnanosti, sociálneho zabezpečenia a sociálnej ochrany

Táto podmienka je osobitne dôležitá pre MO pri riadení ich interného HR procesu. Spracovanie osobitných kategórií osobných údajov je nevyhnutné v každej fáze pracovného vzťahu - od jeho vzniku (proces prijímania nových zamestnancov), jeho vykonaním a zmenami a následne jeho ukončením.

Medzi také príklady, kde by takéto spracovanie mohlo byť nevyhnutné, patrí podávanie práce neschopeniek a ošetrení člena rodiny; presun zamestnanca na vhodnejšiu pozíciu zo zdravotných dôvodov na žiadosť orgánov zdravotnej starostlivosti; dodržiavanie záväzných pravidiel, ktoré zabezpečujú osobitnú ochranu určitých kategórií zamestnancov v prípade ukončenia pracovného pomeru atď.

Všeobecné požiadavky zavedené v GDPR pre aplikácie tohto dôvodu sú:

i) spracovanie musí byť nevyhnutné, aby boli splnené povinnosti správcu údajov, alebo určitého práva dotknutej osoby;

ii) táto povinnosť / právo by sa mala uvádzať v právnych predpisoch EÚ / členských štátov alebo v kolektívnej dohode (vyjednávania);

(iii) Mali by existovať primerané záruky základných práv a záujmov dotknutej osoby.

Na uplatnenie tohto právneho dôvodu je potrebné dodržiavať osobitné vnútroštátne právne predpisy v príslušnom práve členského štátu, v ktorých MO pôsobí ako zamestnávateľ. Vzhľadom na to, že pracovné právo je jednou z oblastí, v ktorých GDPR oprávňuje členské štáty prijať dodatočné právne predpisy týkajúce sa ochrany osobných údajov (článok 88), odporúča sa miestny prístup pre miestne orgány pri uplatňovaní tohto dôvodu.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

3.3. Životne dôležitý záujem dotknutej osoby alebo inej fyzickej osoby

Podobne ako právny dôvod podľa čl. 6, odsek 1, bod "d" GDPR, takáto situácia sa vzťahuje na okolnosti života alebo smrti. Nevyhnutným záujmom by mohla byť dotknutá osoba alebo iná osoba. V porovnaní s čl. 6 je, keď kontrolór nesie bremeno na preukázanie prítomnosti dodatočnej podmienky, a to, že "dotknutá osoba fyzicky alebo právne nie je schopná dať súhlas". Toto znenie znamená, že kontrolór by sa mal najprv pokúsiť získať súhlas dotknutej osoby.

3.4. Spracovanie neziskového subjektu/organizácie s politickým, filozofickým, náboženským alebo odborovým cieľom

Možnosť spracovania citlivých údajov v rámci tohto právneho základu je poskytovaná určitým neziskovým organizáciám, ako sú politické strany, nadácie, cirkvi, iné formy filozofických, náboženských alebo odborových organizácií. Takéto organizácie by mohli spracovávať citlivé údaje, ak:

i) sa tieto údaje týkajú výlučne členov / bývalých členov inštitúcie alebo osôb, ktoré sa s ním pravidelne kontaktujú;

ii) je spracovanie počas ich legitímnej činnosti;

iii) spracovanie prebieha v súvislosti s ich špecifickými účelmi;

iv) existujú primerané záruky pre práva dotknutej osoby;

v) osobné údaje sa nezverejňujú mimo tohto orgánu bez súhlasu dotknutých osôb.

Ďalšie špecifické požiadavky by sa mali požadovať vo vnútroštátnych právnych predpisoch

Tento právny základ by v priebehu svojej činnosti nemal prakticky žiadnu praktickú aplikáciu.

3.5. Dáta sú verejne zverejňované subjektom údajov

Ak sú osobné údaje zjavne zverejnené dotknutou osobou, potom sa predpokladá, že dotknutá osoba upustila od osobitnej ochrany udelenej takýmto informáciám. V každom prípade rozhodnutie o zverejnení takýchto informácií musí byť výsledkom slobodnej voľby jednotlivca. Takéto zverejnenie môže mať rôzne formy - údaje z verejne prístupných registrov, webových stránok, zoznamov, fór alebo dokonca z profilu v sociálnej sieti, ktorá je prístupná bez užívateľského účtu atď. V každom prípade skutočnosť, že takéto údaje sú evidentne zverejnené, nezbavuje prevádzkovateľa povinnosti dodržiavať ostatné požiadavky podľa GDPR - napr .dodržiavanie zásad ochrany údajov, dodržiavanie

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

zásady ochrany súkromia a ochrany súkromia návrhom, prijatie vhodných opatrení na zaručenie bezpečnosti údajov atď.vi

3.6. Zriadenie, výkon alebo obhajoba súdnych pohľadávok / súdov konajúcich v ich súdnej funkcii

V určitých prípadoch môže byť spracovanie citlivých údajov nevyhnutné na kontrolu, uplatnenie alebo obhájenie si právnych nárokov. Riadiaci subjekt nesie bremeno, ktorým preukazuje nevyhnutnosti takého spracovania, t.j. existenciu úzkeho a podstatného spojenia medzi spracovaním a účelmi. Takéto situácie môžu zahŕňať napr. podanie odvolania pred správnymi súdmi o úkonoch vydaných úradmi pre právne úkony, kedy došlo k spracovaniu citlivých údajov v predchádzajúcom správnom konaní; pracovné spory, kde by mali byť zohľadnené zdravotné údaje zamestnancov ako aj zamestnávateľ zo strany miestnych orgánov, atď.

Ďalej by spracovanie takýchto kategórií osobných údajov mohlo byť dokázateľné aj v rámci súdnych činností súdov.

3.7. Základný verejný záujem na základe právnych predpisov EÚ alebo členských štátov

Toto ustanovenie GDPR oprávňuje členské štáty, aby do svojej štátnej legislatívy zaviedli špecifickú hypotézu, v ktorej by sa spracúvali citlivé údaje, ktoré by odôvodňovali takéto spracovanie s významným verejným záujmom.

V každom prípade musia členské štáty v záujme splnenia požiadaviek GDPR zabezpečiť, aby:

i) spracovanie bolo primerané sledovanému cieľu;

ii) sa rešpektovala podstata práva na ochranu údajov;

iii) boli prijaté právne predpisy stanovujúce vhodné a osobitné opatrenia na ochranu základných práv a záujmov dotknutej osoby.

Zostáva odsledovať, ako táto príležitosť bude využitá v budúcnosti. Analýza príslušného miestneho zákona by mala byť vhodná pre miestne orgány, aby sa zistilo, či je možné spoľahnúť sa na uvedené skutočnosti.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

3.8. Preventívne alebo pracovné lekárstvo, hodnotenie pracovnej schopnosti zamestnanca, lekárska diagnostika, poskytovanie zdravotnej alebo sociálnej starostlivosti alebo liečby

Zákaz spracovania osobitných kategórií osobných údajov sa nevzťahuje na spracovanie na účely lekárskej / sociálnej starostlivosti. Takéto spracovanie sa môže realizovať v rôznych oblastiach, ako je napríklad pracovné lekárstvo, lekárska diagnostika alebo poskytovanie služieb v oblasti sociálnej alebo zdravotnej starostlivosti. Takéto spracovanie sa môže uskutočniť buď na základe právnych predpisov EÚ / členských štátov alebo na základe zmluvy so zdravotníckym pracovníkom. Okrem toho, čl. 9, ods. 3 zákona GDPR umožňuje spracovávanie citlivých údajov osobou viazanou povinnosťou zachovávať služobné tajomstvo.

Tento právny dôvod sa vzťahuje na lekárov, zdravotné sestry a iné osoby zapojené do poskytovania služieb zdravotnej starostlivosti.

Z praktického hľadiska by toto ustanovenie umožnilo miestnym orgánom v rámci ich zamestnávateľov zabezpečiť služby v oblasti pracovného lekárstva ako súčasť väčšej povinnosti zabezpečiť pracovné podmienky týkajúce sa zdravia a bezpečnosti.

3.9. Verejný záujem v oblasti verejného zdravia

Podľa Recitálu č. 54 GDPR by sa "verejné zdravie" malo vykladať v súlade s definíciou nariadenia (ES) č. 1338/2008, a to všetkých prvkov týkajúcich sa zdravia, zdravotného stavu vrátane chorobnosti a zdravotného postihnutia, pričom determinanty majú vplyv na zdravotný stav, potreby zdravotnej starostlivosti, zdroje vyčlenené na zdravotnú starostlivosť, poskytovanie a všeobecný prístup k zdravotnej starostlivosti, ako aj výdavky a financovanie zdravotnej starostlivosti a príčiny úmrtnosti.

Dôvodom, ktoré by mohli odôvodniť uplatnenie tohto právneho základu, by mohla byť ochrana pred vážnymi cezhraničnými hrozbami vo veci zdravia alebo zabezpečenie vysokej úrovne kvality a bezpečnosti zdravotnej starostlivosti, zdravotníckych výrobkov alebo zdravotníckych pomôcok.

Spracovanie zdravotných údajov z dôvodov verejného záujmu by nemalo viesť k tomu, že osobné údaje budú spracovávané pre iné účely tretích strán, ako sú zamestnávatelia alebo poisťovne a bankové spoločnosti.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

3.10. Spracovanie na účely archivácie vo verejnom záujme, vedecké alebo historicko-výskumné účely alebo štatistické účely

Spracovanie na tieto účely by malo vychádzať z právnych predpisov členského štátu / EÚ. Spracovanie na tieto účely by malo vychádzať z právnych predpisov členského štátu / EÚ. GDPR vyžaduje, aby legislatívne ustanovenia, ktoré umožňujú takéto spracovanie, boli primerané sledovanému cieľu, rešpektovali podstatu práva na ochranu údajov a ustanovili vhodné a osobitné opatrenia na ochranu základných práv a záujmov dotknutej osoby. Zavedené vii záruky musia zodpovedať citlivej povahe príslušných osobných údajov.

3.11. Ďalšie podmienky v práve členských štátov

Čl. 9 ods. 4 zákona GDPR oprávňuje členské štáty zaviesť ďalšie podmienky alebo obmedzenia na spracovanie určitých osobitných kategórií osobných údajov, a to: genetické údaje, biometrické údaje alebo údaje týkajúce sa zdravia. Preto by sa mala v budúcnosti monitorovať miestna legislatíva uplatniteľná na úrovni miestnej samosprávy a jej orgánov.

4. ZÁVER A PRAKTICKÉ RADY

Miestne orgány by si mali byť vedomé, že určité kategórie osobných údajov si zaslúžia osobitnú ochranu, pretože sú neodmysliteľne spojené s najintímnejšími súkromnými sférami a / alebo predstavujú riziko diskriminácie. Vo všeobecnosti platí, že spracovanie takýchto údajov je zakázané, pokiaľ nie sú prijaté dodatočné podmienky (výnimky z tohto pravidla).

Najpraktickejšie aspekty, ktoré by mohli ovplyvniť aktivity orgánov miestnej samosprávy, sú spracovateľské činnosti údajov o zdraví zamestnancov. GDPR umožňuje takéto spracovanie, ale iba v prípade potreby povinnosti prevádzkovateľa (alebo právo dotknutej osoby) podľa pracovného práva.

Údaje týkajúce sa trestných odsúdení a trestných činov nie sú len osobitnou kategóriou, ale podliehajú aj osobitnému režimu podľa GDPR. Pracovné postupy v oblasti ľudských zdrojov na zhromažďovanie registrov trestov alebo vykonávanie rozsiahlych previerok budúcich zamestnancov by sa mali revidovať vo svetle GDPR.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

5. EXTERNÉ ZDROJE A WEBOWÉ LINKY

Knihy

- **Boardman, R., Mullock, J., Mole, A.** Bird & Bird Guide to General Data Protection Regulation (2016);
- **Ehmann, E., Helfrich, M.** EG Datenschutzrichtlinie: Kurzkommentar, Verlag Dr. Otto Schmidt, Koln, (1999)
- **Voigt, P., von dem Bussche, A.**, The EU General Data Protection Regulation (GDPR) – A Practical Guide, Springer International Publishing (2017);
- **EU** General Data Protection Regulation (GDPR). An Implementation and Compliance Guide, IT Governance Publishing, Cambridgeshire (2016);
- **European** Data Protection. Law and Practice, Executive Editor: Edurado Ustaran, CIPP/E, Partner, Hogan Lovells, IAPP (2018);

Documents of the Article 29 Working Party

- WP29, Guidelines on Consent under Regulation 2016/679, WP 259;
- WP29, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, WP 217;

Web Links

- http://europa.eu/rapid/press-release_IP-18-386_en.htm
- https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en
- https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/sensitive-data/what-personal-data-considered-sensitive_en
- https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/sensitive-data/under-what-conditions-can-my-company-organisation-process-sensitive-data_en

6. REFERENCIE

[i] Voigt, P., von dem Bussche, A., The EU General Data Protection Regulation (GDPR) – A Practical Guide, Springer International Publishing (2017), p. 111.
[ii] Ibid, p. 111.
[iii] Boardman, R., Mullock, J., Mole, A. Bird & Bird Guide to General Data Protection Regulation (2016), p. 18.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

[iv] WP29, Guidelines on Consent under Regulation 2016/679, WP 259, p. 18.
[v] Ibid, p. 18.
[vi] Ibid, p. 113.
[vii] Ibid, p. 115.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

ProLegis

Stanovenie, postavenie a úlohy úradníkov pre ochranu údajov (DPOs)

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

ProLegis

Contents

1. PRÁVNY RÁMEC 4

GDPR 4

2. MENOVANIE DPO 7

2.1. Mandátne menovanie v zmysle GDPR 7

2.1.1. Verejná inštitúcia alebo orgán 7

2.1.2. Hlavné činnosti kontrolóra si vyžadujú pravidelné a systematické monitorovanie dotknutých osôb vo veľkom rozsahu 8

2.1.3. Hlavné činnosti prevádzkovateľa / spracovateľa pozostávajú zo spracovania veľkého rozsahu osobitných kategórií údajov [...] a osobných údajov týkajúcich sa odsúdení a trestných činov v trestnom konaní 9

2.2. Iné okonlnosti pre menovanie DPO 10

2.2.1. Mandatórne menovanie v zmysle práva EU a členského štátu EU 10

2.2.2. Dobrovoľné menovanie 10

2.3. Zmluvné podmienky DPO 11

2.3.1. Pracovná zmluva 11

2.3.2. Zmluva o službe 11

3. POZÍCIA DPO 12

3.1. Zapojenie do všetkých otázok týkajúcich sa ochrany osobných údajov 12

3.2. Zabezpečenie potrebných zdrojov a nezávislosti 12

3.3. Konflikt záujmov 14

4. ÚLOHY DPO 14

4.1. Monitorovanie 14

4.2. DPIA 15

4.3. Kontaktné miesto 15

4.4. Zaznamenávanie údajov 15

5. ZÁVER A PRAKTICKÉ RADY 16

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

6. EXTERNÉ ZDROJE & WEBOVÉ LINKY 17
Bibliografia 17
Dokumenty Článku 29 17
Web Links 17
7. REFERENCIE 17

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

1. PRÁVNY RÁMEC

GDPR

Recitál (97)

Ak spracúvanie vykonáva orgán verejnej moci s výnimkou súdov alebo nezávislých justičných orgánov pri výkone ich súdnej právomoci, alebo ak v súkromnom sektore vykonáva spracúvanie prevádzkovateľ, ktorého hlavnými činnosťami sú spracovateľské operácie, ktoré si vyžadujú pravidelné a systematické monitorovanie dotknutých osôb vo veľkom rozsahu, alebo ak hlavnými činnosťami prevádzkovateľa alebo spracovateľa je spracúvanie osobitných kategórií osobných údajov vo veľkom rozsahu a údajov týkajúcich sa uznania viny za trestné činy a priestupky, mala by prevádzkovateľovi alebo sprostredkovateľovi pri monitorovaní vnútorného dodržiavania tohto nariadenia pomáhať osoba s odbornými znalosťami práva a postupov v oblasti ochrany údajov. V súkromnom sektore sa hlavné činnosti prevádzkovateľa týkajú jeho primárnych činností, a nie spracúvania osobných údajov ako vedľajšej činnosti. Potrebná úroveň odborných znalostí by sa mala určiť najmä v závislosti od vykonávaných operácií spracúvania údajov a od požadovanej ochrany osobných údajov, ktoré spracúva prevádzkovateľ alebo sprostredkovateľ. Takéto zodpovedné osoby, či už sú alebo nie sú zamestnancami prevádzkovateľa, by mali mať možnosť vykonávať svoje povinnosti a úlohy nezávisle.

Článok 37

Určenie zodpovednej osoby

1. Prevádzkovateľ a sprostredkovateľ určia zodpovednú osobu v každom prípade, keď:

(a) spracúvanie vykonáva orgán verejnej moci alebo verejnoprávny subjekt s výnimkou súdov pri výkone ich súdnej právomoci;

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

(b) hlavnými činnosťami prevádzkovateľa alebo sprostredkovateľa sú spracovateľské operácie, ktoré si vzhľadom na svoju povahu, rozsah a/alebo účely vyžadujú pravidelné a systematické monitorovanie dotknutých osôb vo veľkom rozsahu; alebo

(c) hlavnými činnosťami prevádzkovateľa alebo sprostredkovateľa je spracúvanie osobitných kategórií údajov podľa článku 9 vo veľkom rozsahu alebo spracúvanie osobných údajov týkajúcich sa uznania viny za trestné činy a priestupky podľa článku 10.

2. Skupina podnikov môže určiť jednu zodpovednú osobu, ak je zodpovedná osoba ľahko dostupná z každej prevádzkarne.

3. Ak je prevádzkovateľom alebo sprostredkovateľom orgán verejnej moci alebo verejnoprávny subjekt, pre viaceré takéto orgány alebo subjekty sa môže určiť jedna zodpovedná osoba, pričom sa zohľadní ich organizačná štruktúra a veľkosť.

4. V iných prípadoch, ako sú prípady uvedené v odseku 1, zodpovednú osobu môže určiť alebo, ak sa to vyžaduje v práve Únie alebo v práve členského štátu, určí prevádzkovateľ alebo sprostredkovateľ alebo združenia a iné subjekty zastupujúce kategórie prevádzkovateľov alebo sprostredkovateľov. Zodpovedná osoba môže konať v mene takýchto združení a iných subjektov zastupujúcich prevádzkovateľov alebo sprostredkovateľov.

5. Zodpovedná osoba sa určí na základe jej odborných kvalít, a to najmä na základe jej odborných znalostí práva a postupov v oblasti ochrany údajov a na základe spôsobilosti plniť úlohy uvedené v článku 39.

6. Zodpovedná osoba môže byť členom personálu prevádzkovateľa alebo sprostredkovateľa, alebo môže plniť úlohy na základe zmluvy o poskytovaní služieb.

7. Prevádzkovateľ alebo sprostredkovateľ zverejnia kontaktné údaje zodpovednej osoby a oznámia ich dozornému orgánu.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

Článok 38

Postavenie zodpovednej osoby

1. Prevádzkovateľ a sprostredkovateľ zabezpečia, aby bola zodpovedná osoba riadnym spôsobom a včas zapojená do všetkých záležitostí, ktoré súvisia s ochranou osobných údajov

2. Prevádzkovateľ a sprostredkovateľ podporujú zodpovednú osobu pri plnení úloh uvedených v článku 39, a to tak, že poskytujú zdroje potrebné na plnenie týchto úloh a prístup k osobným údajom a spracovateľským operáciám, ako aj zdroje na udržiavanie jej odborných znalostí.

3. Prevádzkovateľ a sprostredkovateľ zabezpečia, aby zodpovedná osoba v súvislosti s plnením týchto úloh nedostávala žiadne pokyny. Prevádzkovateľ ani sprostredkovateľ ju nesmú odvolať alebo postihovať za výkon jej úloh. Zodpovedná osoba podlieha priamo najvyššiemu vedeniu prevádzkovateľa alebo sprostredkovateľa.

4. Dotknuté osoby môžu kontaktovať zodpovednú osobu v súvislosti so všetkými otázkami týkajúcimi sa spracúvania ich osobných údajov a uplatňovania ich práv podľa tohto nariadenia.

5. Zodpovedná osoba je v súvislosti s výkonom svojich úloh viazaná povinnosťou zachovávať mlčanlivosť alebo dôvernosť informácií v súlade s právom Únie alebo s právom členského štátu.

6. Zodpovedná osoba môže plniť iné úlohy a povinnosti. Prevádzkovateľ alebo sprostredkovateľ zabezpečia, aby žiadna z takýchto úloh alebo povinností neviedla ku konfliktu záujmov.

Článok 39

Úlohy úradníka pre ochranu údajov

1. Úradník pre ochranu údajov má aspoň tieto úlohy:

a) informovať prevádzkovateľa alebo spracovateľa a zamestnancov, ktorí vykonávajú svoje povinnosti podľa tohto nariadenia a iných ustanovení Únie alebo členských štátov týkajúcich sa ochrany údajov;

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

b) monitorovať súlad s týmto nariadením, inými ustanoveniami Únie alebo členského štátu o ochrane údajov as politikami prevádzkovateľa alebo spracovateľa v súvislosti s ochranou osobných údajov vrátane pridelenia zodpovednosti, zvyšovania povedomia a odbornej prípravy zamestnancov zapojených do operácií spracovania a súvisiacich auditov;

c) poskytovať poradenstvo, ak je o to požiadané, pokiaľ ide o hodnotenie vplyvu ochrany údajov a monitorovať jeho výkonnosť podľa článku 35;

d) spolupracovať s orgánom dohľadu;

e) konať ako kontaktné miesto pre dozorný orgán v otázkach súvisiacich so spracovaním vrátane predchádzajúcej konzultácie uvedenej v článku 36 av prípade potreby konzultovať s ohľadom na akúkoľvek inú záležitosť.

2. Úradník pre ochranu údajov pri výkone svojich úloh náležite zohľadní riziko spojené so spracovateľskými operáciami, pričom zohľadní povahu, rozsah, kontext a účely spracovania.

2. MENOVANIE DPO

2.1. Mandátne menovanie v zmysle GDPR

2.1.1. Verejná inštitúcia alebo orgán

GDPR neobsahuje právnu definíciu, čo možno rozumieť pod pojmami "verejný orgán alebo orgán". Či sa jedná o určitú fyzickú / právnickú osobu, alebo verejný orgán / orgán, mal by byť definovaný v zmysle štátnych legislatívnych predpisov každého príslušného členského štátu. Tento pojem by sa mal vykladaný v širšom kontexte a v každom prípade zahŕňať aj národné, regionálne a **miestne orgány**. Podľa WP29 však môže zahŕňať aj určité fyzické / právnické osoby, ktorých činnosť je riadená verejným / súkromným právom (napr. Verejná doprava, zásobovanie vodou a energiou, cestná infraštruktúra, verejnoprávne vysielanie, verejné bývanie alebo disciplinárne orgány pre regulované povolanie). Logika takejto interpretácie spočíva v tom, že občania (subjekty údajov) majú obmedzenú voľbu, či a akým spôsobom sú ich osobné údaje spracúvané. Hoci takáto interpretácia nie je povinná a záväzná, odporúča sa dôkladné posúdenie a analýza v rámci týchto organizácií, či sa má vymenovať DPO.

Treba poznamenať, že WP29 odporúča v zmysle dobrej praxe vymenovať úradníka pre ochranu údajov, ktorého funkcie by mali zahŕňať aj všetky vykonané operácie spracovania vrátane tých, ktoré nesúvisia s plnením verejnej úlohy alebo vykonávaním

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

službnej povinnosti (napr. zamestnanci). Žiadne ustanovenie GDPR však nevyžaduje vymenovanie úradníka pre ochranu údajov iba za spracovateľské činnosti súvisiace s verejnými funkciami. Preto rozumnejší a bezpečnejší výklad je, že LA vymenuje DPO, ktorý je **zodpovedný za všetky činnosti spracovania údajov v rámci organizácie** (vzťahy s občanmi, zamestnancami, kandidátmi na prácu, bývalými zamestnancami, inými verejnými orgánmi atď.).

2.1.2. Hlavné činnosti kontrolóra si vyžadujú pravidelné a systematické monitorovanie dotknutých osôb vo veľkom rozsahu

Činnosti spracúvania údajov spoločnosti MO by všeobecne spadali do rozsahu pôsobnosti bodu 2.1.1. vyššie, t. j. MO by mal vymenovať úradníka pre ochranu údajov na základe svojej schopnosti orgánu verejnej moci / orgánu. V záujme zrozumiteľnosti sa bude realizovať stručná analýza dvoch ďalších hypotéz v rámci GDPR, kde je uložená povinnosť vymenovať úradníka pre ochranu údajov. Tieto informácie by mohli byť užitočné pre súkromné subjekty, ktorých základné imanie je čiastočne alebo úplne vo vlastníctve obce alebo iných orgánov štátnej správy / štátu a ktoré nepatria do pôsobnosti "verejného orgánu / orgánu".

Pod pojmom **"hlavné činnosti"** sa rozumejú kľúčové operácie potrebné na dosiahnutie cieľov kontrolóra alebo spracovateľa. Medzi príklady uvedené vo WP29 patrí spracovanie zdravotných záznamov v nemocniciach alebo sledovanie vykonávané súkromnou bezpečnostnou spoločnosťou. V rovnakej dobe sú štandardné aktivity zamestnancov IT podpory vylúčené z "hlavných aktivít" organizáciei.

Koncept **"veľkého rozsahu"** nie je explicitne definovaný v GDPR. Výslovne sa uvádza, že spracovanie na regionálnej, národnej alebo nadnárodnej úrovni, ktorá zahŕňa značné množstvo údajov a ktoré by mohlo mať vplyv na veľký počet dotknutých osôb a ktoré by pravdepodobne viedlo k vysokému riziku, by sa mohlo považovať za spracovanie "vo veľkom meradle". Práve naopak jediní lekári, ako napríklad jednotliví zdravotnícki odborníci alebo právnici, nespracúvajú osobné údaje "vo veľkom meradle".

Podľa WP29 neúplný zoznam činností, ktoré možno považovať za spracovanie vo veľkom rozsahu, zahŕňa:

- spracovanie údajov pacientov nemocnicou;
- spracovávanie cestovných údajov jednotlivcov pomocou systému mestskej hromadnej dopravy (napríklad sledovanie prostredníctvom cestovných kariet);

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

- spracovanie geografických údajov zákazníkov medzinárodného reťazca rýchleho občerstvenia v reálnom čase na štatistické účely spracovateľom špecializovaným na poskytovanie týchto služieb;
- spracovanie údajov o zákazníkoch poisťovňou / bankou;
- spracovanie osobných údajov pre behaviorálnu reklamu prostredníctvom vyhľadávača
- spracovanie údajov (obsah, návštevnosť, lokalizácia) telefonickými alebo internetovými poskytovateľmi služieb[ii].

Pojem **"pravidelný"** je neodmysliteľne spojený so spracovaním, ktoré sa uskutočňuje buď trvalo (neustále) alebo pravidelne. Pojem "systematické monitorovanie" vyžaduje, aby sa spracovanie uskutočňovalo v rámci určitého systému v rámci určitého plánu, stratégie alebo podobnej vopred definovanej metodológie. Medzi príklady patria okrem iného prevádzkovatelia telekomunikačných sietí, profilovanie, behaviorálna reklama, inteligentné zariadenia atď.

2.1.3. Hlavné činnosti prevádzkovateľa / spracovateľa pozostávajú zo spracovania veľkého rozsahu osobitných kategórií údajov [...] a osobných údajov týkajúcich sa odsúdení a trestných činov v trestnom konaní

Pre pojmy "hlavné činnosti" a "veľké" pozri bod 2.1.2. vyššie.

Tento výraz by sa mal interpretovať korektívne ako "alebo". Inými slovami, akékoľvek spracovanie, ktoré zahŕňa buď spracovanie osobitných kategórií údajov alebo osobné údaje týkajúce sa odsúdení a trestných činov v trestných veciach, ktoré sú vo veľkom rozsahu a sú súčasťou hlavnej činnosti organizácie, by malo vyžadovať vymenovanie DPO.

Špeciálne kategórie údajov sú:

• osobné údaje odhaľujúce rasový alebo etnický pôvod;

· politické názory;

· náboženské alebo filozofické presvedčenie;

· členstvo v odboroch;

· genetické údaje;

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

· biometrické údaje na účely jednoznačnej identifikácie fyzickej osoby:

· údaje týkajúce sa zdravia alebo údajov týkajúcich sa sexuálneho života alebo sexuálnej orientácie fyzickej osoby.

Osobné údaje týkajúce sa odsúdení a trestných činov v trestných veciach môžu obsahovať informácie obsiahnuté v rozsudkoch súdu, v registri trestov, v úkonoch vyšetrovacích orgánov.

2.2. Iné okonlnosti pre menovanie DPO

2.2.1. Mandatórne menovanie v zmysle práva EU a členského štátu EU

- Podľa čl. Podľa článku 37 ods. 4 smernice o ochrane ľudských práv a základných slobôd je EÚ a / alebo sú členské štáty oprávnené stanoviť iné situácie, kedy sa vymenovanie úradníka pre ochranu údajov považuje za povinné. Takéto povinné vymenovanie môže byť požadované kvalitatívnym označením (napr. v prípade niektorých spracovateľských činností špecifických pre daný sektor) alebo kvantitatívnym označením (napr. V prípade, že organizácia spracováva osobné údaje určitých dotknutých osôb s údajmi z viacerých čísel). Napríklad Nemecko vo svojich právnych predpisoch o ochrane osobných údajov zaviedlo širšie požiadavky ako GDPR:

i) spoločnosti, ktoré podnikajú v Nemecku a zamestnávajú najmenej 10 osôb v oblasti automatizovaného spracovania budú mať povinnosť vymenovať úradníka pre ochranu údajov;

ii) v prípade automatizovaného spracovania v rámci podnikania na účel prevodu; anonymizovaný prevod; trhu alebo stanoviska, v takom prípade spoločnosti musia vymenovať úradníka pre ochranu údajov bez ohľadu na počet osôb zamestnaných na automatizované spracovanie osobných údajov [iii].

2.2.2. Dobrovoľné menovanie

GDPR tiež ustanovuje možnosť dobrovoľne vymenovať DPO. Takýto prístup by mohol byť prijateľný pre organizácie, ktoré chcú preukázať dodržiavanie pravidiel ochrany údajov a podporiť transparentnosť a dôveru. Keďže činnosť miestnych orgánov by skôr spadala pod prvú povinnú požiadavku (verejný orgán / orgán), dobrovoľné vymenovanie by sa uplatňovalo v prípade niektorých organizácií, ktorých základné imanie vlastní obec / štát, napr. podniky verejnej dopravy, verejné školy / univerzity, verejní poskytovatelia verejných služieb (voda, plyn, elektrická energia) atď.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

2.3. Zmluvné podmienky DPO

2.3.1. Pracovná zmluva

V GDPR sa výslovne ustanovuje možnosť vymenovať úradníka pre ochranu údajov na základe pracovnej zmluvy. To znamená dve možnosti: (i) vymenovať niekoho, kto už pracuje v organizácii, aby spojil svoju funkciu s funkciami DPO, alebo (ii) odhaliť novú pracovnú pozíciu pre DPO. Voľba medzi týmito dvoma možnosťami závisí v podstate od štruktúry, počtu zamestnancov, pracovného zaťaženia a druhu a počtu činností spracovania údajov a mala by sa vykonávať od prípadu k prípadu. Ak je príslušná organizácia spoločnosti LA pomerne malá (napr. Nachádza sa v malej dedine s obmedzeným počtom občanov, ktorých údaje sa spracovávajú), mohlo by byť rozumné nepristúpiť k novému zamestnancovi, ale rozdeliť funkciu úradníka pre ochranu údajov na niekoho, kto už pracuje (v každom prípade by sa mal zabrániť konfliktu záujmov). Naopak, ak je miestna organizácia obrovská a / alebo jej každodenné aktivity súvisia so spracovaním značného množstva osobných údajov (alebo citlivých údajov / údajov týkajúcich sa odsúdení a trestných činov), voľba otvoriť novú pozíciu pre (aspoň jeden úradník pre ochranu údajov by sa zdal opodstatnený.

2.3.2. Zmluva o službe

GDPR nezaväzuje organizácie na vymenovanie úradníkov pre ochranu údajov iba ako zamestnancov. V nariadení je ustanovené, že funkcia úradníka pre ochranu údajov sa môže zadávať externému subjektu / organizácii na základe zmluvy o poskytovaní služieb. WP29 odporúča, aby externé tímy úradníkov pre ochranu údajov disponovali kvalitnou praxou, aby mali poverený kontakt vedúceho a osobu zodpovednú za každého klienta, ktorá by mala byť uvedená v zmluve o poskytovaní služieb. Okrem toho každý člen externej organizácie DPO by mal spĺňať všetky uplatniteľné požiadavky podľa GDPR.

OutsourcingAutsorsing funkcií DPO na externé organizácie by mohol byť primeranou voľbou, pretože táto organizácia by mala potrebnú úroveň odborných vedomostí, skúseností a udržiavať všetky príslušné certifikácie.

V neposlednom rade, v závislosti od miestneho práva, uzavretie zmluvy o poskytovaní služieb s externým úradníkom pre ochranu údajov vyžaduje vykonávanie určitých formálnych postupov (napríklad podľa zákona o verejnom obstarávaní).

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

3. POZÍCIA DPO

3.1. Zapojenie do všetkých otázok týkajúcich sa ochrany osobných údajov

GDPR výslovne stanovuje, že úradník pre ochranu údajov by mal byť zapojený do všetkých otázok týkajúcich sa ochrany osobných údajov v organizácii. WP29 vidí zapojenie úradníka pre ochranu údajov (pokiaľ ide o konzultácie, poradenstvo, kontrolu atď.) V každom procese, ktorý zahŕňa spracovanie osobných údajov od najskoršieho možného štádia ako jeden z nástrojov na zabezpečenie ochrany súkromia podľa návrhuiv.

V každom procese, ktorý zahŕňa spracovanie osobných údajov od najskoršieho možného štádia ako jeden z nástrojov na zabezpečenie ochrany súkromia už v štádiu návrhu.

Praktické dôsledky zapojenia DPO do organizácie by mohli zahŕňať napríklad:

· účasť na pracovných stretnutiach (WP29 predpisuje/žiada účasť na stretnutiach vedúceho a stredného manažmentu, ale v praxi by interakcia DPO s personálom na expertnej úrovni mohla mať podobnú (ak nie vyššiu) pridanú hodnotu);

· požadujú sa konzultácie s úradníkom pre ochranu údajov vždy, keď sa prijme rozhodnutie o riadení;

· Hľadanie konzultácií s úradníkom na ochranu údajov, ktoré opatrenia sa majú vykonať, v prípade porušenia údajov.

3.2. Zabezpečenie potrebných zdrojov a nezávislosti

Úrad pre ochranu údajov nemôže správne vykonávať svoju funkciu, ak nebude mať k dispozícii potrebné zdroje. Vedenie organizácie je preto zodpovedné za to, aby zabezpečil, že úradník pre ochranu údajov je riadne zabezpečený minimálne z týchto hľadísk.

- **Organizačné záležitosti:**

  o Úrad pre ochranu údajov by mal mať tím, ktorý by im pomohol pri plnení svojich funkcií. To je dôležité najmä pre väčšie organizácie. V niektorých prípadoch by mohlo byť riešením aj vyšší počet úradníkov pre ochranu údajov.

  o Prístup do všetkých ostatných tímov v organizácii. Úrad pre ochranu údajov nemôže správne vykonávať svoje funkcie, ak dochádza k nesprávnej komunikácii so všetkými

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

ostatnými tímami, ktoré zodpovedajú za spracovanie údajov (napr. Oddelenie pre registráciu a uchovávanie súborov, právne oddelenie, ľudské zdroje, účtovníctvo, oddelenie IT atď.);

o Zodpovedný iba pred najvyšším vedením. GDPR výslovne stanovuje, že úradník pre ochranu údajov by sa mal zodpovedať iba najvyššiemu riadeniu organizácie. Pre MO by to mal byť úrad napr. starostu, alebo by mohlo ísť o obecnú radu, riaditeľa / predsedu príslušnej správnej jednotky atď. Táto požiadavka je veľmi dôležitá z hľadiska zabezpečenia nezávislosti úradníka pre ochranu údajov. Ak by bol vzťah DPO s vedením nepriamy (napr. Prostredníctvom sprostredkovateľov, ako je napríklad vedúci oddelenia pre právne služby alebo oddelenie ľudských zdrojov), úradník pre ochranu údajov by nemohol riadne vykonávať svoje funkcie, pretože by sa mohol ocitnúť v situácii, keď je úradník pre ochranu údajov zodpovedný niekomu, DPO by mal vykonávať kontrolu.

o Čas na vykonanie funkcie. Táto požiadavka by sa mala dodržiavať najmä v prípadoch, ak je úradník pre ochranu údajov vymenovaný na prácu na čiastočný úväzok, alebo ide o externého úradníka pre ochranu údajov, ktorý okrem iných povinností vykonáva aj ochranu údajov. WP29 predpisuje ako správnu prax stanovenie percenta času pre funkciu DPO, ak sa nevykonáva na plný úväzok.

- **Finančné záležitosti**
- Úradník pre ochranu údajov by mal mať potrebné finančné zdroje na vykonávanie svojich funkcií. Ak organizácia nezabezpečí dostatočný rozpočet na aktivity na ochranu údajov, mohol by sa ohroziť riadny výkon funkcií DPO.
- Úradník pre ochranu údajov by mal mať potrebné vybavenie (miestnosti, počítače, internetové pripojenie, databázy, technické riešenia, ako sú softvérové programy atď.).

Záležitosti v oblasti vzdelávania – úroveň odborných znalostí DPO by sa mala neustále zvyšovať (prostredníctvom kurzov, zabezpečovaním novej literatúry atď.).Vzhľadom na skutočnosť, že ochrana údajov je veľmi dynamickou oblasťou ľudského poznania, je pochopiteľné, že úradník pre ochranu údajov by sa mal oboznamovať s aktuálne najnovšími trendmi a vývojom, aby bolo možné riadne zabezpečiť najvyššiu možnú úroveň z hľadiska ochrany údajov v a čeliť najnovším výzvam z hľadiska technologického a právneho rozvoja.

Dôležitým aspektom nezávislosti úradníka pre ochranu údajov je zákaz sankcionovania / spôsobenia akýchkoľvek nepriaznivých dôsledkov na vykonávanie ich úloh. Nepriaznivé

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

dôsledky by sa mohli líšiť v závislosti od širokého spektra situácií - od prepustenia, alebo iného druhu disciplinárneho trestu až po odmietnutie povýšenia, odopretie dávok získaných inými zamestnancami, atď. Možno očakávať, že členské štáty zavedú zmeny a doplnenia do svojej pracovnej legislatívy a zabezpečia ochranu úradníkov pre ochranu údajov pred prepustením počas obdobia výkonu svojich funkcií a určitého obdobia.

Zároveň by sa mala urobiť primeraná interpolácia tohto zákazu - úradník pre ochranu údajov nemôže byť potrestaný za riadne vykonávanie svojich služieb. Ak však úradník pre ochranu údajov nemá potrebné vedomosti a zručnosti, dochádza k disciplinárnemu porušeniu atď., Organizácie by mali byť schopné ich odmietnuť na základe všetkých dôvodov prepustenia

3.3. Konflikt záujmov

Ak je úradník pre ochranu údajov menovaný na základe pracovnej zmluvy, toto označenie by nemalo mať za následok konflikt záujmov. Konflikt záujmov by mohol vzniknúť, ak má DPO v rámci organizácie inú funkciu, ktorá určuje účel a prostriedky na spracovanie údajov v rámci daného interného procesu. Inak povedané, úradník pre ochranu údajov nemôže byť súčasne riaditeľom, výkonným riaditeľom, vedúcim pôsobenia, šéfom financií, hlavným lekárom, vedúcim oddelenia marketingu, vedúcim oddelenia ľudských zdrojov alebo vedúcim oddelení IT. Okrem toho by iné funkcie v organizačnej štruktúre mohli spôsobiť konflikt záujmov, ak tieto pozície alebo úlohy vedú k určeniu cieľov a prostriedkov spracovania (napríklad účtovník, právny poradca, špecialista na IT).

Ku konfliktu záujmov môže dôjsť nielen v prípade menovania úradníka pre ochranu údajov na základe pracovnej zmluvy, ale aj v prípade externého úradníka pre ochranu údajov. Ak by bol úradník pre ochranu údajov vyzvsný, aby zastupoval správcu alebo spracovateľa pred súdmi v prípadoch týkajúcich sa ochrany údajov, vznikne tak konflikt záujmov, pretože kontrolór a spracovateľ majú protichodné záujmy.

4. ÚLOHY DPO

4.1. Monitorovanie

Jednou z kľúčových úloh úradníka pre ochranu údajov je sledovanie všetkých činností spracovania údajov v rámci organizácie. Neodmysliteľne sa spája s prijímaním / zhromažďovaním informácií, vnútornou analýzou týchto informácií a objasňovaním, odporúčaniami a poskytovaním poradenstva v rámci organizácie. Monitorovacia funkcia je zameraná na interné procesy v rámci organizácie, preto by mal byť informovaný nielen manažment, ale aj riadni zamestnanci na expertnej úrovni, ktorých povinnosti súvisia so spracovaním osobných údajov.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

4.2. DPIA

GDPR ustanovuje, že úradník pre ochranu údajov by mal byť zapojený do DPIA s poradnými funkciami. Pracovná skupina WP29 odporúča ako osvedčenú prax požiadať radu DPO o stanovisko k jednému alebo viacerým z nasledujúcich otázok, ktoré sa týkajú posúdenia vplyvu:

- či vôbec vykonať DPIA;
- akú metodiku treba dodržiavať pri vykonávaní DPIA;
- či má DPIA vykonávať interne alebo ho externe;
- aké bezpečnostné opatrenia (vrátane technických a organizačných opatrení) uplatňovať na zmiernenie akýchkoľvek rizík týkajúcich sa práv a záujmov dotknutých osôb
- či bolo posúdenie vplyvu na ochranu údajov vykonané správne a či jeho závery sú v súlade s GDPR.v.

Ak sa manažment organizácie rozhodne odchýliť od odporúčania DPO ako súčasť zásady zodpovednosti, je vhodné, aby toto rozhodnutie a jeho zdôvodnenie boli zdokumentované a aby bol schopný predložiť túto dokumentáciu orgánom vykonávajúcim dohľad v prípade auditu.

4.3. Kontaktné miesto

DPO je hlavným kontaktným miestom orgánov dohľadu (článok 39 ods. 1, položka "e" GDPR) a dotknutých osôb (článok 38 ods. 4 GDPR), pokiaľ ide o akékoľvek záležitosti týkajúce sa ochrany údajov v rámci organizácia. Preto je mimoriadne dôležité správne oznamovať kontaktné údaje DPO dozornému orgánu a dotknutým osobám. Okrem toho požiadavka na poskytnutie kontaktných údajov o úradníkovi pre ochranu údajov je jedným z prvkov zásady transparentnosti podľa čl. 12, 13 a 14 GDPR.

Žiadne ustanovenie v GDPR nebráni tomu, aby úradník pre ochranu údajov dostal príležitosť požiadať o radu od orgánov dohľadu, pokiaľ ide o akýkoľvek problém súvisiaci s ochranou údajov v rámci organizácie.

4.4. Zaznamenávanie údajov

Hoci povinnosť uchovávať záznamy o spracovateľských činnostiach je poskytovaná len pre kontrolórov a spracovateľov a nie pre úradníkov pre ochranu údajov, nič v GDPR nebráni organizáciám prideliť túto funkciu DPO. Úlohy úradníka pre ochranu údajov uvedené v GDPR sú len minimálne stanovené, takže organizácie môžu slobodne

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

delegovať iné úlohy na DPO. WP29 považuje pridelenie povinnosti uchovávania záznamov DPO ako jeden z nástrojov umožňujúcich úradníkovi pre ochranu údajov vykonávať svoje úlohy kontroly na dodržiavanie predpisov, informovanie a poskytovanie poradenstva kontrolórovi / spracovateľovi. Keďže záznam je účinným nástrojom na zabezpečenie zodpovednosti, bolo by rozumné delegovať túto povinnosť na úradníka pre ochranu údajov.

5. ZÁVER A PRAKTICKÉ RADY

DPO je jedným z kľúčových členov pri zabezpečovaní súladu s novými pravidlami na ochranu údajov. Význam tejto úlohy vo veľkej miere závisí od samotnej organizácie. Ak sa organizácia riadne zaoberá úradníkom pre ochranu údajov vo všetkých otázkach ktoré súvisia s ochranou údajov a zabezpečuje potrebné zdroje na to, aby úradník pre ochranu údajov mohol vykonávať svoje funkcie, DPO by mohlo byť jedným z rozhodujúcich faktorov na zabezpečenie rovnováhy a dbať na posilnenie dôvery vrámci spoločnosti. V prípade, že by to tak nebolo, úradník pre ochranu údajov by sa chápal ako iluzívna figúrka, ktorá by nemala skutočné funkcie, iba riadiť komunikáciu týkajúcu sa ochrany údajov, čo nie je myšlienka tejto úlohy v rámci GDPR.

Orgány miestnej samosprávy by mali byť povzbudzované k tomu, aby ustanovili kvalifikovaných úradníkov pre ochranu údajov, čo sa môže považovať za náročnú úlohu vzhľadom na nedostatok pripravovaných jednotlivcov na úrovni EÚ. V každom prípade bude v nasledujúcich rokoch povinnosťou určiť, ako sa bude vyvíjať úloha úradníka pre ochranu údajov. V každom prípade by bolo priaznivé pre spoločnosť, ak MO by bolo jedným z priekopníckych príkladov, pokiaľ ide o to, ako najlepšie využiť postavenie DPO.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

6. EXTERNÉ ZDROJE & WEBOVÉ LINKY

Bibliografia

- **Harting, N.** Datenschutz-Grundverordnung: Das neue Datenschutzrecht in der betrieblichen Praxis, Verlag Dr. Otto Schmidt KG, Köln, 2016;
- **Voigt, P., von dem Bussche, A.** The EU General Data Protection Regulation (GDPR) – A Practical Guide, Springer International Publishing (2017);
- **Boardman, R., Mullock, J., Mole, A.** Bird & Bird Guide to General Data Protection Regulation (2016);
- **EU** General Data Protection Regulation (GDPR). An Implementation and Compliance Guide, IT Governance Publishing, Cambridgeshire (2016);

Dokumenty Článku 29

- WP29, Guidelines on Data Protection Officers ('DPOs'), WP 243 rev.01;

Web Links

- http://europa.eu/rapid/press-release_IP-18-386_en.htm
- https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en
- ….

7. REFERENCIE

[i] Ibid, p. 6-7.
[ii] Ibid, p. 8.
[iii] Demmel, A. The New German Federal Data Protection Act, Squire Patton Boggs, URL: <https://www.squirepattonboggs.com/~/media/files/insights/publications/2017/09/the-new-german-federal-data-protection-act/27836--german-federal-data-protection-alert.pdf> (26.03.2018);
[iv] WP29, Guidelines on Data Protection Officers ('DPOs'), WP 243 rev.01, p. 13.
[v] Ibid, p.17.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

ProLegis

Posúdenie vplyvu ochrany

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

ProLegis

Contents

1. Νομικό πλαίσιο 3
   1.1. Γενικός Κανονισμός για την Προστασία Δεδομένων (GDPR ή ΓΚΠΔ)..... 3
2. Πότε είναι απαραίτητη μια ΕΑΠΔ? 5
   2.1. Βασικά..... 5
   2.2. Περιπτώσεις στις οποίες η ΕΑΠΔ είναι επιτακτική..... 6
      2.2.1. Περαιτέρω σκέψεις σχετικά με την ανάγκη διενέργειας μιας ΕΑΠΔ 6
      2.2.2. Διενέργεια μιας ΕΑΠΔ για πολλά παρόμοια συστήματα επεξεργασίας δεδομένων 7
      2.2.3. Θετικοί και αρνητικοί κατάλογοι για την ΕΑΠΔ..... 7
   2.3. Χρόνος διενέργειας της ΕΑΠΔ..... 7
   2.4. Επανεξέταση της ΕΑΠΔ 8
   2.5. Διαβούλευση με την αρχή προστασίας δεδομένων σύμφωνα με το άρθρο 36 του ΓΚΠΔ 9
3. Ποιος είναι υπεύθυνος για τη διενέργεια μιας ΕΑΠΔ;..... 9
   3.1. Βάση 9
   3.2. Συμμετοχή στην ΕΑΠΔ..... 10
4. Πώς διενεργείται μια ΕΑΠΔ..... 10
   4.1. Βάση 10
   4.2. Εφαρμογή μιας ΕΑΠΔ 11
   4.3. Ελάχιστο περιεχόμενο μιας ΕΑΠΔ 11
   4.4. Η επεξεργασία ΕΑΠΔ..... 12
   4.5. Συμπερίληψη των υποκειμένων των δεδομένων και των εκπροσώπων τους .. 14
   4.6. Η έκθεση σχετικά με την εφαρμογή εκτίμησης αντικτύπου για την προστασία της ιδιωτικότητας..... 15
5. Συμπεράσματα και πρακτικές συμβουλές..... 17
6. Εξωτερικές πηγές και σύνδεσμοι 17
   6.1. Βιβλία και άρθρα 17
   6.2. Αρχεία Working Party Άρθρου 29..... 18
   6.3. Διαδικτυακοί σύνδεσμοι..... 18

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

1. Právny rámec

1.1. General Data Protection Regulation (GDPR)

Článok 35

Posúdenie vplyvu na ochranu údajov

1. Ak typ spracúvania, najmä s využitím nových technológií a s ohľadom na povahu, rozsah, kontext a účely spracúvania pravdepodobne povedie k vysokému riziku pre práva a slobody fyzických osôb, prevádzkovateľ pred spracúvaním vykoná posúdenie vplyvu plánovaných spracovateľských operácií na ochranu osobných údajov. Pre súbor podobných spracovateľských operácií, ktoré predstavujú podobné vysoké riziká, môže byť dostatočné jedno posúdenie.

2. Prevádzkovateľ sa počas vykonávania posúdenia vplyvu na ochranu údajov radí so zodpovednou osobou, pokiaľ bola určená.

3. Posúdenie vplyvu na ochranu údajov uvedené v odseku 1 sa vyžaduje najmä v prípadoch:

(a) systematického a rozsiahleho hodnotenia osobných aspektov týkajúcich sa fyzických osôb, ktoré je založené na automatizovanom spracúvaní vrátane profilovania a z ktorého vychádzajú rozhodnutia s právnymi účinkami týkajúcimi sa fyzickej osoby alebo s podobne závažným vplyvom na ňu,

(b) spracúvania vo veľkom rozsahu osobitných kategórií údajov podľa článku 9 ods. 1 alebo osobných údajov týkajúcich sa uznania viny za trestné činy a priestupky podľa článku 10, alebo

(c) systematického monitorovania verejne prístupných miest vo veľkom rozsahu.

4. Dozorný orgán vypracuje a zverejní zoznam tých spracovateľských operácií, ktoré podliehajú požiadavke na posúdenie vplyvu na ochranu údajov podľa odseku 1. Dozorný orgán zasiela tieto zoznamy výboru uvedenému v článku 68.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

5. Dozorný orgán môže stanoviť a zverejniť aj zoznam spracovateľských operácií, v prípade ktorých sa nevyžaduje posúdenie vplyvu na ochranu údajov. Dozorný orgán zasiela tieto zoznamy výboru.

6. Príslušný dozorný orgán pred prijatím zoznamov uvedených v odsekoch 4 a 5 uplatní mechanizmus konzistentnosti uvedený v článku 63, ak takéto zoznamy zahŕňajú spracovateľské činnosti, ktoré súvisia s ponukou tovaru alebo služieb dotknutým osobám alebo sledovaním ich správania vo viacerých členských štátoch, alebo ak môžu podstatne ovplyvniť voľný pohyb osobných údajov v rámci Únie.

7. Posúdenie obsahuje aspoň:

(a) systematický opis plánovaných spracovateľských operácií a účely spracúvania, vrátane prípadného oprávneného záujmu, ktorý sleduje prevádzkovateľ,

(b) posúdenie nutnosti a primeranosti spracovateľských operácií vo vzťahu k účelu,

(c) posúdenie rizika pre práva a slobody dotknutých osôb uvedeného v odseku 1 a

(d) opatrenia na riešenie rizík vrátane záruk, bezpečnostných opatrení a mechanizmov na zabezpečenie ochrany osobných údajov a na preukázanie súladu s týmto nariadením, pričom sa zohľadnia práva a oprávnené záujmy dotknutých osôb a ďalších osôb, ktorých sa to týka.

8. Pri posudzovaní dosahu spracovateľských operácií vykonávaných relevantnými prevádzkovateľmi alebo sprostredkovateľmi sa náležite sleduje, či títo prevádzkovatelia alebo sprostredkovatelia dodržiavajú schválené kódexy správania uvedené v článku 40, a to najmä na účely posúdenia vplyvu na ochranu údajov.

9. Prevádzkovateľ sa podľa potreby usiluje získať názory dotknutých osôb alebo ich zástupcov na zamýšľané spracúvanie bez toho, aby bola dotknutá ochrana obchodných alebo verejných záujmov alebo bezpečnosť spracovateľských operácií.

10. Ak má spracúvanie podľa článku 6 ods. 1 písm. c) alebo e) právny základ v práve Únie alebo v práve členského štátu, ktorému prevádzkovateľ podlieha, a toto právo upravuje konkrétnu spracovateľskú operáciu alebo súbor daných operácií, a posúdenie vplyvu na ochranu údajov sa už vykonalo v rámci všeobecného posúdenia vplyvu v súvislosti s prijatím tohto právneho základu, odseky 1 až 7 sa neuplatňujú, pokiaľ členské štáty nepovažujú za potrebné vykonať takéto posúdenie pred začatím spracovateľských činností.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

11. V prípade potreby prevádzkovateľ vykoná prehodnotenie s cieľom posúdiť, či sa spracúvanie uskutočňuje v súlade s posúdením vplyvu na ochranu údajov, a to aspoň vtedy, keď došlo k zmene rizika, ktoré predstavujú spracovateľské operácie.

Recitály 89 do 96:

Článok 35 GDPR je úzko spojený s článkami 24, 25 a 32. Hlavným rozdielom medzi článkom 32 a článkom 35 je, že článok 32 (Bezpečnosť spracúvania údajov) sa zameriava na riziká spojené s nepriaznivými udalosťami, ako sú útoky, zatiaľ čo *Vplyv na ochranu osobných údajov* (DPIA), ktorý je založený na článku 35 sa **zameriava predovšetkým na riziká vyplývajúce z pravidelného spracovania údajov**.

DPIA je dôležitým nástrojom na zavádzanie ochrany údajov technologickými prostriedkami (ochrana údajov v štádiu návrhu), ako sa uvádza v článku 25 ods. 1. Oba sú založené na zásade predbežnej opatrnosti, tj identifikácii rizík už v počiatočných fázach návrhu, kde sa zvážia príslušné protiopatrenia pred zavedením a uvedením do prevádzky systémov spracovania údajov.

DPIA je nástroj na identifikáciu a analýzu týchto rizík. V prípadoch, keď nie je DPIA povinná, je potrebné vykonať analýzu súvisiacich rizík, aby sa primerane vykonávali ustanovenia článku 25 a článku 32. Obidve nariadenia sa výslovne týkajú práv a slobôd fyzických osôb. Hĺbka a požadovaná dokumentácia analýzy rizík, ktorá sa má vykonať, závisí od zložitosti a rizikovej miery spracovania. Odporúčame písomne predložiť dokumentáciu o analýze rizík. Implementácia princípu ochrany údajov podľa návrhu prekračuje riziká, ktoré boli vopred identifikované v najnovšej analýze rizík a obsahuje rozhodnutia, ktoré sa v neskoršom štádiu ad hoc realizovali vývojári systému (inžinierske systémy) pri vykonávaní zásad minimalizácie údajov.

2. Kedy sa vyžaduje DPIA[1]?

2.1. Základné informácie

DPIA sa musí vykonať pred spracovaním osobných údajov, ktoré nesú vysoké roziko práv a slobôd fyzických osôb.

[1]Nasledujúci text sa významne zakladá na publikácii v nemeckom jazyku Kastelitz, M., Hötzendorfer, W., Riedl, R., Ausgewählte Fragen der Durchführung einer Datenschutz-Folgenabschätzung gemäß Art 35 DSGVO, Jahrbuch Datenschutzrecht 2017, 113ff.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

V podstate sa DPIA musí vykonávať pre akúkoľvek formu spracovania údajov, ak sa nedá určiť a priori, že práva a sobody fyzických osôb nie sú ovpúlyvnené konkrétnou operáciou pre spracovanie údajov.

Pre aký typ spracovania údajov je potrebné takéto riziko predpokladať, napr. stanovených v bodoch uvedených v článku 35 ods. 3 alebo v odôvodnení 91. Dôraz sa kladie na používanie takzvaných nových technológií, vágneho právneho konceptu zavedeného v GDPR, pokiaľ ide o DPIA. Posúdenie rizika musí nielen zohľadniť existujúce rizikové konštelácie, ale aj pravdepodobnosť budúcich udalostí, ktoré sa majú identifikovať v prognostickom hodnotení. Výsledky hodnotenia musia byť zdokumentované..

Článok 35 ods. 1 posledná veta v spojení s odôvodnením 92 poskytuje dôležitý pohľad na posúdenie potreby DPIA: "Za určitých okolností môže byť primerané a ekonomicky vhodné, aby sa nepoužilo hodnotenie vplyvu na súkromie len na Ak chce verejné orgány alebo iné verejné orgány vytvoriť spoločnú platformu na aplikáciu alebo spracovanie, alebo keď viacero zúčastnených strán chce zaviesť spoločné aplikačné alebo spracovateľské prostredie pre celý podnikateľský sektor, na trhu segmentu alebo rozšírenej horizontálnej činnosti..

2.2. Prípady, v ktorých je DPIA povinná/záväzná

Čl. 35 Odd 3 obsahuje záväzné prípady použitia DPIA:

(a) systematické a rozsiahle hodnotenie osobných aspektov, ktoré sa týkajú fyzických osôb, a tie ktoré sú založené na automatizovanom spracovaní vrátane profilovania, a na ktorých sa zakladajú rozhodnutia, majúce právne účinky, ktoré sa týkajú fyzickej osoby,a lebo ktoré významne ovplyvňujú fyzickú osobu;

(b) spracovanie veľkého rozsahu osobitných kategórií údajov uvedených v článku 9 ods. 1 alebo osobných údajov týkajúcich sa odsúdení a trestných činov uvedených v článku 10; alebo

(c) systematické monitorovanie verejne prístupnej oblasti vo veľkom meradle.

2.2.1. Ďalšie úvahy týkajúce sa potreby realizovať DPIA

V odôvodnení 91 sa uvádzajú ďalšie prípady vyžadujúce DPIA:

Operácie spracovania

a) ktoré potenciálne zahŕňajú veľký počet ľudí a / alebo vysokú mieru rizika a / alebo využívanie rozsiahlej technológie v súlade s najnovšími technológiami;

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

b) ktoré zahŕňajú vysokú mieru rizika a sťažujú subjektom údajov, aby si uplatňovali svoje práva;

c) ak sa osobné údaje spracovávajú pri prijímaní rozhodnutí o konkrétnych fyzických osobách po systematickom a rozsiahlom hodnotení osobných aspektov týkajúcich sa fyzických osôb na základe profilovania týchto údajov alebo po spracovaní osobitných kategórií osobných údajov, biometrických údajov alebo údajov o trestné odsúdenia a trestné činy alebo súvisiace bezpečnostné opatrenia;

d) ktoré predstavujú vysokú mieru rizika, pretože bránia dotknutým osobám vo výkone práva alebo využívania služby alebo plnenia zmluvy;

e) ktoré predstavujú vysoké riziko, pretože obsahujú systematický veľký rozsah

2.2.2. Vykonávanie DPIA pre niekoľko podobných systémov na spracovanie údajov

V článku 35 ods. 1 sa uvádza, že pre systémy spracovania s podobnou úrovňou rizika sa môže vykonať jednotná DPIA. Pri posudzovaní takejto podobnosti sa musí zvážiť celkový účel spracovania údajov v každom jednotlivom prípade. V odôvodnení 92 sa uvádza, že vzhľadom na hospodárske náklady môže mať DPIA širší tematický rozsah, vďaka čomu majú členovia v konkrétnom odvetví alebo v segmente trhu možnosť pokryť aplikácie alebo spracovateľské prostredie alebo široko zdieľané horizontálne postupy s jediným DPIA.

2.2.3. Pozitívne a negatívne zoznamy DPIA

Možno predpokladať, že regulačné agentúry zverejnia pozitívne / negatívne zoznamy, ktoré povedú k rozhodnutiu, či sa v konkrétnom prípade vyžaduje DPIA. Tieto zoznamy definujú typy spracovania vyžadujúce DPIA ("pozitívne zoznamy") a prípady, keď sa nevyžaduje DPIA ("negatívne zoznamy"). Obidva zoznamy musia národné regulačné orgány zasielať Európskej rade pre ochranu údajov ako súčasti režimu regulačnej súdržnosti (článok 35 ods. 4) s cieľom zabezpečiť lepšiu harmonizáciu v celej EÚ.

Treba poznamenať, že pracovná skupina zriadená podľa článku 29 (WP/PS29) odporúča vykonať DPIA aj v prípadoch, kde sa zdá byť nejasné, či je potrebné, aby sa DPIA prispelo k splneniu právnych požiadaviek na riadnu ochranu údajov.

2.3. Načasovanie DPIA

Načasovanie a metóda, ktoré sa uplatňujú na DPIA, stanovuje správca. Predpokladajú sa právne sankcie v prípade nevykonania DPIA. Odporúča sa začať prípravu na DPIA v najskoršom možnom štádiu projektu. Každé oddelenie alebo príslušní zamestnanci, ktorí

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

sa podieľajú na spracovaní údajov, musia iniciovať príslušné procesy. Školenie sa odporúča preto, aby sa zvýšila informovanosť o potrebe DPIA v rámci organizácie

Zváženie opatrení na minimalizáciu rizika v počiatočnom štádiu akéhokoľvek projektu vrátane spracovania údajov, môže pomôcť udržať byrokratické úsilie na pomerne nízkej úrovni.

DPIA môže usmerňovať vyhľadávanie adekvátnych riešení a môže pomôcť implementovať - ako už bolo spomenuté vyššie - požiadavky na ochranu údajov efektívne a včas prostredníctvom vhodných technologických riešení (ochrana údajov podľa návrhu) a výberu predvolených nastavení s ohľadom na ochranu údajov.

Za predpokladu komplexných a intenzívnych príprav DPIA bude usmerňovať plánovaný projekt od fázy skorých nápadov až po jeho konečné operatívne vykonávanie a preukáže iterakčný charakter procesu DPIA.

Či sa DPIA požadovalo pre spracovanie činností, ktoré boli účinné pred všeobecnou platnosťou GDPR (25. mája 2018), je otvorená otázka. Prijatím doslovného znenia ("pred") sa vyžaduje DPIA len pre procesy, ktoré začali fungovať po 25. máji 2018 alebo ktoré po tomto dátume prechádzajú značnými zmenami..

Keďže v týchto prípadoch systém spracovania údajov už funguje, predbežná kontrola nie je možná. Okrem toho tieto operácie neexistujú v neregulovanom priestore (za predpokladu, že boli zohľadnené všetky právne predpisy a požiadavky na podávanie správ z predchádzajúceho právneho rámca).

Napriek tomu PS/WP29 dôrazne odporúča formu DPIA pre spracovateľské systémy, ktoré sa už používajú, aby sa predišlo právnej neistote a dokonca aj právnym sankciám.

2.4. Posúdenie DPIA

Po vykonaní DPIA je potrebné vykonať aj revíziu-prehodnotenie navrhovaných opatrení, ak sa to považuje za potrebné. Možno považovať za nevyhnutné preskúmanie samotného spracovania údajov na identifikáciu akýchkoľvek nových prvkov rizík súvisiacich so spracovaním údajov. V odôvodnení 89 sa uvádza, že po prvom posúdení môže byť potrebná revízia DPIA v primeranom čase. Pri vykonávaní protokolu DPIA by mal byť súčasťou dokumentácie časový rámec pre rutinné kontroly alebo budúce obnovy.

Treba zvážiť technologický vývoj, novú právnu úpravu a zmeny v spracovateľských postupoch. Ak dôjde k riziku, musí sa uzavrieť nová zmluva DPIA.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

Povinnosť vykonávať DPIA je súčasťou povinnosti kontrolóra údajov, ktorý dokumentuje ich zodpovednosť. Dokumentácia a správa by nemali poskytovať iba informácie o vykonávanom DPIA, ale mali by uvádzať všetky dôvody, prečo nebolo predprípravu kompletného DPIA, alebo ukončenia DPIA po zistení vysokých rizík vzhľadom na dotknuté osoby.

2.5. Konzultácia s orgánom na ochranu osobných údajov podľa Čl. 36 GDPR

Prevádzkovateľ uskutoční s dozorným orgánom pred spracúvaním konzultácie (DPA), ak by DPIA odhalila závažné riziká a prevádzkovateľ by nevedel, ako prijať akékoľvek nápravné opatrenia na zmiernenie takýchto rizík. DPA musí reagovať na túto žiadosť o konzultáciu do štrnástich týždňov. Pri komplexných a inovatívnych projektoch sa odporúča začať DPIA v najskoršom možnom štádiu, takže akékoľvek odporúčania DPIA môžu byť zohľadnené pri realizácii plánu projektu.

3. Kto zodpovedá za riadenie DPIA?

3.1. Základné informácie

Zodpovednosť za vykonávanie smernice DPIA je v právomoci prevádzkovateľa - v tomto prípade je to miestny verejný orgán. Najprv návrh Komisie prevzal/presunul zodpovednosť za DPIA spracovateľovi údajov, ktorý koná podľa príkazu prevádzkovateľa. Naopak, odôvodnenie 95 sa obmedzuje na nárok na spracovateľa, aby pomohol správcovi, ak je to potrebné a na požiadanie, pri zabezpečovaní dodržiavania povinností, ktoré vyplývajú z posúdenia vplyvu ochrany údajov.

V praxi bude vhodné zmluvne požadovať, aby bol spracovateľ, ktorý je k dispozícii, aby bol zapojený do aktívnej podpory počas celého procesu DPIA. Toto je tiež nad rámec článku 28 ods. 3 písm. F), v ktorom sa ustanovuje, že zmluva o spracovaní (alebo iný právny nástroj) by mala poskytnúť spracovateľovi, berúc do úvahy povahu spracovania aj informácie, ktoré má k dispozícii, dodržiavanie povinností vyplývajúcich z článkov 32 až 36. Často iba spracovateľ disponuje potrebnými informáciami na posúdenie príslušných aspektov spracovania. Pritom sa musí brať do úvahy riziko zverejnenia obchodných a obchodných tajomstiev. Opäť sa odporúča konkrétne zmluvné nariadenie. Ak sa predpokladá spracovanie údajov spoločnými kontrolórmi, DPIA v zmysle čl. 35, ods. 1, ods. 2, môže byť vykonané aj jedným z riadiacich jednotiek - ktorý nevypúšťa ostatných zodpovedných kontrolórov

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

3.2. Účasť v DPIA

DPIA by sa mal organizovať ako projekt a ako taký by mal byť vybavený potrebnými materiálnymi a ľudskými zdrojmi zodpovedajúcim vysokým stupňom riadenia. Pri zostavovaní projektového tímu je potrebné venovať osobitnú pozornosť komplexnosti projektu, požadovaným odborným znalostiam a potrebným znalostiam o konkrétnom projekte a jeho prostredí. V praxi môže byť vytvorený tím právnikov, IT pracovníkov, CISO, úradník pre ochranu údajov, oddelenie, ktoré požiadalo o spracovanie ("vlastník údajov") atď.

Osobitná pozornosť sa venuje zabezpečeniu a forme predchádzania konfliktom záujmov. Tí, ktorí sa v budúcnosti zaoberajú spracovaním údajov, sa nemusia považovať za nezávislých, ale na druhej strane môžu poskytnúť cenný prínos pre vypracovanie hodnotenia vplyvu na súkromie. Implementáciu môže vykonávať interný tím, ako aj externé tretie strany. V ideálnom prípade by mal byť zapojený aj nezávislý orgán.

Kontrolór sa musí poradiť s úradníkom pre ochranu údajov. V súlade s článkom 39 ods. 1 písm. C) poradenstvo, ktoré sa týka DPIA a monitoruje sa vykon, ktorý patrí medzi zákonné povinnosti DPO, avšak len na požiadanie a nie na pre tých na vedúcej pozícii.

Preto je povinnosťou kontrolóra získať poradenstvo úradníka pre ochranu údajov. V akej dobe a do akej miery musí byť pracovník ochrany údajov zapojený do procesu, je to na rozhodnutí správcu. Následné preskúmanie záverečnej správy by bolo postačujúce. V praxi sa dôrazne odporúča včas zapojiť úradníka pre ochranu údajov, hlavne kvôli jeho odbornosti.

V závislosti od organizácie kontrolóra je vhodné, aby bola DPIA schválená na úrovni riadenia alebo zodpovedajúcim autorizovaným orgánom.

4. Ako zaobchádzať s DPIA

4.1. Základné informácie

x 1. Je potrebné zdôrazniť, že GDPR nepredpisuje žiadnu konkrétnu formu ani konkrétnu metódu navrhovania hodnotenia vplyvu na ochranu údajov, o ktorej sa v súčasnosti intenzívne diskutuje na vnútroštátnej a európskej úrovni. WP29 uvádza, že na podporu implementácie ustanovení GDPR možno použiť rôzne možnosti návrhu a odkazuje na

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

príklady existujúcich modelov procesov DPIA (všeobecných alebo sektorových) v prílohe 1.[2]

4.2. Implementácia DPIA

Prevádzkovateľ je v podstate slobodný v tom, ako má vykonávať proces DPIA a môže ho prispôsobiť existujúcim vnútorným postupom za predpokladu, že miestna verejná autorita/orgán zohľadní štyri požiadavky uvedené v článku 35 ods. 7 smernice GDPR a) d) ako minimálne požiadavky DPIA, ktoré podrobnejšie opisuje pracovná skupina zriadená podľa článku 29 a okrem toho berie do úvahy bod "zainteresované strany" (pozri článok 35 ods. 2) a názory dotknutých osôb [pozri článok 35 ods. 9]):

a) systematický opis zamýšľaných spracovateľských operácií a účel spracovania vrátane prípadného oprávneného záujmu kontrolóra;

b) posúdenie nevyhnutnosti a proporcionality spracovateľských operácií vo vzťahu k účelom;

c) posúdenie rizík týkajúcich sa práv a slobôd dotknutých osôb uvedených v odseku 1; a

d) opatrenia plánované na riešenie rizík vrátane bezpečnostných opatrení, bezpečnostných opatrení a mechanizmov na zabezpečenie ochrany osobných údajov a na preukázanie súladu s týmto nariadením s prihliadnutím na práva a oprávnené záujmy dotknutých osôb a iných dotknutých osôb.

4.3. Minimálny obsah DPIA

Článok 35 ods. 7 písm. A) až d) GDPR v súvislosti s odôvodneniami 84 a 90 vyžaduje minimálne:

a) systematický opis zamýšľaných spracovateľských operácií a účel spracovania vrátane prípadného oprávneného záujmu kontrolóra;

b) posúdenie nevyhnutnosti a proporcionality spracovateľských operácií vo vzťahu k účelom;

c) posúdenie rizík týkajúcich sa práv a slobôd dotknutých osôb uvedených v odseku 1; a

2 WP29, WP 248, 15: Different methodologies (see Annex 1 of WP248 for examples of data protection and privacy impact assessment methodologies) could be used to assist in the implementation of the basic requirements set out in the GDPR (Annex 1).

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

d) opatrenia plánované na riešenie rizík vrátane bezpečnostných opatrení, bezpečnostných opatrení a mechanizmov na zabezpečenie ochrany osobných údajov a na preukázanie súladu s týmto nariadením s prihliadnutím na práva a oprávnené záujmy dotknutých osôb a iných dotknutých osôb.

Písmená c) a d) sú prejavmi tzv. "Prístupu založeného na riziku" GDPR, ktoré sú relevantné nielen pri implementácii DPIA, ale aj v kontexte článkov 24, 25 a 32 GDPR. Inými slovami, DPIA je špecifickým príkladom prístupu založeného na riziku pri spracovávaní údajov, v krátkosti ide o údaje, o ktorých sa predpokladá, že predstavujú vysoké riziko pre práva a slobody fyzických osôb, a žiada o rozsiahlejšie hodnotenie rizika a liečbu. V zásade však takéto hodnotenie rizika zahŕňa aj akúkoľvek ďalšiu kontrolu prípustnosti spracovania údajov vrátane adekvátnych technických a organizačných opatrení, ktoré minimalizujú riziko pred ich zavedením (pozri len článok 24 ods. 1 GDPR).

4.4. Proces DPIA

DPIA by sa malo vnímať ako proces (nielen ako správa), ktorý by sa mal začať čo najskôr ovplyvniť návrh predmetu ("projekt"). V dôsledku toho sa hodnotenie vplyvu líši aj od auditu, ktorý vyhodnocuje projekt ex-post a zvyčajne príde neskoro na to, aby "vyrovnal" potreby ochrany údajov, ktoré by DPIA mala produkovať.

Teraz existuje množstvo návrhov na implementáciu procesu DPIA, ktorý sa podobným spôsobom podobá výsledkom štúdie PIAF (2012), v ktorej sa zmapovali metodiky hodnotenia vplyvu na súkromie v siedmich krajinách (vrátane derivácie "najlepšej praxe" odporúčania a hlavné prvky procesu hodnotenia vplyvu na súkromie) okrem iného pre Komisiu EÚ. Boli identifikované nasledujúce základné prvky:

1. Určenie, či je potrebné PIA (prahová analýza).
2. Identifikácia tímu PIA a stanovenie referenčného rámca.
3. Opis navrhovaného projektu [a identifikácia zainteresovaných strán].
4. Analýza informačných tokov a iných dopadov na súkromie.
5. Konzultácie so zainteresovanými stranami.
6. Riadenie rizík [Identifikácia rizík a možných riešení].
7. Kontrola dodržiavania právnych predpisov.
8. Formulovanie odporúčaní.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

9. Príprava a zverejnenie správy [napr. Na webovej stránke organizácie].

10. Realizácia odporúčaní.

11. Externá kontrola a / alebo audit tretej strany.

12. Prehodnotenie PIA, ak sa príslušný projekt zmení [Aktualizácia PIA v prípade zmien v projekte].

Model DPIA pre inteligentné siete a inteligentné meracie systémy, ktorý je výslovne uvedený v odporúčaní Európskej komisie 2014/724 / EÚ, stanovuje tieto kroky:[3]

1. Krok 1 Predbežné hodnotenie a kritériá určujúce potrebu vykonať DPIA.

2. Krok 2 Začatie.

3. Krok 3 Identifikácia, charakterizácia a opis inteligentných sieťových systémov / aplikácií spracúvajúcich osobné údaje.

4. Krok 4 Identifikácia príslušných rizík.

5. Krok 5 Posúdenie rizika ochrany údajov.

6. Krok 6 Identifikácia a odporúčanie kontrol a zvyškových rizík.

7. Krok 7 Dokumentácia a vypracovanie správy DPIA.

8. Krok 8 Preskúmanie a údržba

Nová norma ISO / IEC 29134 poskytuje usmernenia pre proces vykonávania posúdení vplyvu na súkromie a pre štruktúru a obsah správy PIA. Proces je rozdelený na nasledovné štyri čiastkové procesy:

1. Prahová analýza.

2. Príprava PIA.

3. Vykonajte PIA.

4. Kontrola PIA.

3 Commission Recommendation 2014/724/EU of 10 October 2014 on the Data Protection Impact Assessment Template for Smart Grid and Smart Metering Systems, ABl L 2014/300, 63.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

V ktorom bode a v koľkých častiach je proces DPIA rozdelený, je to vec výberu, ďalšie návrhy sa pohybujú napríklad v troch alebo štyroch fázach v šiestich až siedmich fázach. Skôr sa za dôležité považuje zrozumiteľná štruktúra a priebeh procesu, ktorý zohľadňuje najmä požiadavky čl. 35 (7) GDPR a odporúčania pracovnej skupiny zriadenej podľa článku 29.

4.5. Začlenenie dotktnutých osôb alebo ich zástupcov

Podľa článku 35 ods. 9 správca údajov, ak je to vhodné, skúma názory dotknutých osôb alebo ich zástupcov na zamýšľané spracovanie bez toho, aby bola dotknutá ochrana obchodného alebo verejného záujmu alebo bezpečnosť spracovateľských operácií. Zahrnutie slova "podľa potreby" v súvislosti s rokovaniami o trialógu spôsobuje, že nie je jasné, za akých okolností by sa konkrétne malo získať postavenie dotknutej osoby alebo jej zástupcu a v akých prípadoch (prípustné) to možno upustiť.

Spôsob, akým sa požaduje stanovisko, je citlivá na kontext a WP29 uznáva rôzne spôsoby, ako je vykonanie štúdie (internej alebo externej), formálne rozhovory so zástupcami zamestnancov alebo odborových zväzov a predloženie dotazníka budúcim zákazníkom radič. Zo samotného znenia je možné vyvodiť len stanovisko (v pôvodnej verzii stanovísk komisie), nie však povinnosť brať do úvahy alebo dokonca požiadavku (nového) súhlasu (nad rámec zákona o ústavnej zmluve (ArbVG)) zamestnaneckej rady ako zástupca dotknutých osôb. Napriek tomu sa kontrolór bude musieť zaoberať stanoviskami dotknutých osôb alebo ich zástupcami a bude sa ich musieť zaoberať v hodnotení vplyvu. Či združenia na ochranu spotrebiteľa môžu byť zahrnuté pod pojem "zástupca", je kontroverzná v literatúre[4].

V každom prípade sa povinnosť konzultovať ***výslovne*** bez toho, aby bola dotknutá ochrana obchodných alebo verejných záujmov alebo bezpečnosť operácií spracovania. Preto prevádzkovateľ môže v extrémne obmedziť alebo odmietnuť povinnosť poskytnúť dotknutým osobám alebo zástupcom informácie o zamýšľanom spracovaní podľa článku 35 ods. 9 (čo v tomto prípade povedie k tomu, že a priori zapojenie do článok 35 ods. 9 nie je možný, keďže existencia dostatočných informácií je sine qua non pre stanovisko príslušných osôb alebo ich zástupcov).

4 *Martini* in Paal/Pauly (Hrsg), Datenschutz-Grundverordnung (2016) Art 35 Rz 60; dagegen (mangels rechtlicher Verbundenheit) *Laue/Nink/Kremer*, Das neue Datenschutzrecht in der betrieblichen Praxis (2016) 245 Rz 99.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

Pri vykonávaní hodnotenia vplyvu ochrany údajov sa v správe odporúča zdokumentovať dôvody, prečo nebolo získané žiadne alebo len obmedzené obsahové stanovisko, alebo získané stanovisko nebolo alebo len čiastočne bolo zohľadnené.

4.6. Správa o vykonávaní hodnotenia vplyvu na súkromie

Treba poznamenať, že správa DPIA nie je skutočným cieľom DPIA, ale "prostriedkom na ukončenie" dokumentácie procesu (interného a externého). Správa by sa nemala podceňovať - dokumentuje implementáciu a výsledky a z dôvodov súladu sa treba vyhnúť pouhým "správam PRDPIA". Správa môže tiež slúžiť ako sprievodca a kontrolný zoznam pri vykonávaní DPIA.

Art. 35 GDPR obsahuje, trochu prekvapujúco, žiadnu výslovnú požiadavku na prípravu správy o vykonávaní DPIA. Skutočnosť, že pre prevádzkovateľa existuje povinnosť dokumentácie, je nepochybne a implicitne vyplýva z článku 35 ods. 7 GDPR a tiež z článku 5 ods. 2 GDPR (zodpovednosť) v spojení s článkom 24 ods. 1 GDPR a článkom 36 ods. 3 písm. E) (ktorý vyžaduje, aby orgán dohľadu poskytol "posúdenie vplyvu ochrany údajov uvedené v článku 35"). Preskúmanie požadované v článku 35 ods. 11 na posúdenie, či sa spracovanie vykonáva v súlade s DPIA, a či vyžaduje, aby sa výsledky hodnotenia vplyvu zachovali. Okrem toho podávanie správ o realizovaných PIA je v súlade s celosvetovou osvedčenou praxou v tejto oblasti (pozri časť IV.1.

Proces DPIA sa dopĺňa s dokumentáciou v zmysle "živého dokumentu", pričom sa začína dokumentáciou analýzy prahovej hodnoty v prípade, že nie je potrebné vykonať DPIA. Aj keď táto analýza dokazuje, že DPIA nie je potrebná a proces je prerušený, zodpovedný za jej zodpovednosť a dôkazy bude zodpovedný kontrolór. Táto písomná dokumentácia môže byť predložená dozornému orgánu v každom budúcom procese a bude sledovať interné úvahy a hodnotenia.

Pokiaľ ide o obsah, správa DPIA v podstate stanovuje postup (vrátane prezentácie faktov v zmysle systematického popisu celého predmetu testu - "cieľ hodnotenia") a výsledkov procesu DPIA. Tak ako v prípade samotného procesu DPIA, GDPR nestanovuje žiadne osobitné pravidlá pre vypracovanie správy DPIA. Avšak ako minimálny obsah sú vopred stanovené kritériá uvedené v pracovnej skupine na ochranu údajov podľa článku 29 v prílohe 2 k WP 248, ktoré sú v podstate založené na článku 35 ods. 7. ISO / IEC 29134 odporúča nasledujúci obsah správy o hodnotení vplyvu na súkromie s dôrazom na hodnotenie rizika:

1. Príslušné požiadavky na ochranu súkromia.
2. Opis rozsahu.
3. Opis použitých kritérií rizika.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

4. Účastníci implementácie.
5. Konzultované zainteresované strany.

Toto sa potvrdzuje aj odôvodnením č.90, v ktorom sa o.i.uvádza:" Toto posúdenie vplyvu by malo zahŕňať predovšetkým opatrenia, záruky a mechanizmy plánované na zmiernenie tohto rizika, zabezpečnie ochrany osobných údajov a preukázať súlad s týmto nariadením."

V podrobnej štúdii PIAF je minimálny obsah správy PIA náaseldovný: [5]

1. Úvod a základné informácie vrátane toho, kto vykonal PIA, jej kontaktné údaje a kde nájsť ďalšie informácie a ďalšie zdroje pomoci a poradenstva
2. Opis projektu, informačných tokov a vplyvov na súkromie.
3. Výsledky konzultácií so zainteresovanými stranami
4. Opis fázy posúdenia rizika a zmierňovania rizika vrátane zvažovaných alternatív.
5. Analýza dodržiavania právnych predpisov.
6. Odporúčania.
7. Prílohy, ak je to potrebné.

V prípade, že je k dispozícii správa alebo konečný návrh, môže nastať otázka, čo sa má robiť so zodpovednou (vnútornou) osobou, a to predovšetkým či a kým ju má schváliť - prakticky relevantný bod, ktorý zostane nezmenený GDPR. ICO vo svojom Kódexe pravidiel výslovne stanovuje nasledovné: "[o] udržiať vhodné podpisy v rámci organizácie". Keďže zodpovedná osoba musí vykonať DPIA, z toho vyplýva, že do DPIA sú zapojení príslušne poverení zástupcovia zodpovednej osoby a majú aj konečnú zodpovednosť. Úroveň riadenia bude mať zvyčajne konečnú rozhodovaciu právomoc nad predmetom a povahou projektu DPIA. Ako minimálny variant by mal manažér projektu alebo úradník pre ochranu údajov podávať správy na "najvyššej riadiacej úrovni", ako je ustanovené v čl. 38 (3) GDPR.

GDPR nie je povinná uverejňovať DPIA, ale WP29 odporúča jeho publikovanie (aspoň čiastočne) s cieľom zvýšiť dôveru v spracovanie údajov a podporiť transparentnosť. Publikácia sa odporúča najmä v prípadoch, keď časť ("plánované") spracovanie ovplyvní časť verejnosti.

5 *De Hert/Kloza/Wright* (Hrsg), PIAF, Recommendations for a privacy impact assessment framework for the European Union, Deliverable D3 (2012) 31, http://piafproject.eu/ref/PIAF_D3_final.pdf.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

5. Záver a praktické typy

Predovšetkým regulačné agentúry s kvalitnými zdrojmi vyvinuli vlastné prístupy pre hodnotenie vplyvu na súkromie v priebehu niekoľkých rokov. Z dnešnej perspektívy možno očakávať, že orgány pre ochranu údajov, ktoré už vyvinuli svoj vlastný model, budú uprednostňovať alebo šíriť to, hlavne preto, že znalosti príslušného dozorného orgánu o ich vlastných odporúčaniach budú najvýraznejšie. Obsah aktuálne dostupných modelov vnútroštátnych orgánov dohľadu (z členských štátov EÚ) je často pred GDPR a nie je (zatiaľ) dôsledne prispôsobený požiadavkám alebo terminológii GDPR.

Medzinárodná organizácia pre medzinárodnú spoluprácu (ICO) však pridala do svojho štandardu PIA (2014) správu "Veľké údaje, umelej inteligencie, strojové učenie a ochrana údajov" (požiadavky na čítanie) a terminológiu GDPR, orgánov. Je potrebné zistiť, či Európska rada pre ochranu údajov (článok 68) poskytne usmernenia, odporúčania a / alebo osvedčené postupy pre DPIA v súlade s čl. 70 ods. 1 písm. E).

Odporúčania na prvý pohľad:

- Dokumentácia všetkých rozhodnutí, najmä dôvod, pre ktorý nebol vykonaný DPIA (ak je to vhodné);
- Ak máte pochybnosti, vykonajte DPIA:
- Zapojenie interných a externých zainteresovaných strán;
- Používanie modelov, osvedčených postupov a, ak je to vhodné podobných DPIA už existujúcich
- Publikovanie DPIA:
  - najmä verejnými orgánmi;
  - zvyšuje informovanosť o ochrane súkromia a zvyšuje dôveru.

6. Externé zdroje a webové linky

6.1. Bibliografia a literatúra

- ***Kastelitz, M., Hötzendorfer, W., Riedl, R***., Ausgewählte Fragen der Durchführung einer Datenschutz-Folgenabschätzung gemäß Art 35 DSGVO, Jahrbuch Datenschutzrecht 2017, 113ff.
- ***De Hert, Paul/Kloza, Dariusz/Wright, David,*** Recommendations for a privacy impact assessment framework for the European Union http://www.piafproject.eu/ref/PIAF_D3_final.pdf
- ***Wright, David/De Hert, Paul*** **(Ed.),** Privacy Impact Assessment, Springer Science & Business Media, Dordrecht, Heidelberg, London, New York 2012

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

- ***De Hert/Kloza/Wright*** (Ed.), **PIAF**, Recommendations for a privacy impact assessment framework for the European Union, Deliverable D3 (2012), http://piafproject.eu/ref/PIAF_D3_final.pdf; more available at http://piafproject.eu/Deliverables.html.
- ***Martini in Paal/Pauly*** (Ed.), Datenschutz-Grundverordnung (2016) Art 35 Rz 60; dagegen (mangels rechtlicher Verbundenheit) Laue/Nink/Kremer, Das neue Datenschutzrecht in der betrieblichen Praxis (2016) 245 Rz 99.

6.2. Dokumenty článku 29 Working Party – pracovná časť/strana

- Artikel-29-Working Party, WP 248, April 4, 2017: Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679 http://ec.europa.eu/newsroom/document.cfm?doc_id=44137
- WP 248, as last Revised and adopted on 4 October 2017 (rev.01): Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679 https://www.dsb.gv.at/documents/22758/112500/Guidelines_on_Data_Protection_Impact_Assessment_(DPIA).pdf/ed5daa8c-d388-43a6-9842-629b8175a99c

6.3. Webové Linky

- Brussels Laboratory for Data Protection and Privacy Impact Assessments http://www.vub.ac.be/LSTS/dpialab/
- ICO, Big data, artificial intelligence, machine learning and data protection (2017), 99 f, https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

ProLegis

Transparentnosť

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

ProLegis

Contents

1. PRÁVNY RÁMEC 4
   1.1. Zmluvy Európskej únie 4
   1.2. Charta základných práv EU 4
   1.3. GDPR 4
2. VÝZNAM TRANSPARENTNOSTI PODĽA GDPR 6
   2.1. Súčasti transparentnosti v zmysle GDPR (Čl. 12) 6
      2.1.1. “Stručné, prehľadné, zrozumiteľné a ľahko dostupné” 6
      2.1.2. “Jasný a jednoduchý jazyk“ 6
      2.1.3. Spôsob poskytovania informácií (Čl. 12, ods.1 a ods 5 “bez poplatku”). 7
   2.2. Informácie poskytované dotknutým osobám (Čl.13 a Čl.14) 7
      2.2.1. Aké informácie poskytnúť? 7
      2.2.3 Ako majú byť informácie poskytnuté? 8
      2.2.4. Kedy poskytnúť informácie? 9
      2.2.5. Kedy upozorniť na zmeny transparentnosti informácií, ktoré by mali byť poskytnuté kontrolórmi údajov? 9
   2.3. Metódy 10
      2.3.1. Upozornenia o ochrane osobných údajov 10
      2.3.2. “Push” & “pull” notices 10
      2.3.3. Iné typy “vhodných opatrení “ 10
      2.3.4. Vizualizácia 11
   2.4. Výkonnosť práv dotknutých osôb 11
      2.4.1. Výnimky z povinnosti poskytovať právo na informácie 11
3. ZÁVER A PRAKTICKÉ RADY 12
4. EXTERNÉ ZDROJE a WEBLINKy 13
Bibliografia 13

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

Dokumenty Článku 29 - Pracovná časť 13
Webové Linky 13
5. REFERENCES 13

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

1. PRÁVNY RÁMEC

1.1. Zmluvy Európskej únie

Článok 1 Zmluvy o EÚ -> prijaté rozhodnutia "čo najotvorenejšie a čo najbližšie k občanom";

Článok 11 (2) Zmluvy o EÚ -> "Inštitúcie udržiavajú otvorený, transparentný a pravidelný dialóg s reprezentatívnymi združeniami a občianskou spoločnosťou";

Článok 15 Zmluvy o fungovaní Európskej únie -> občania Únie, ktorí majú právo na prístup k dokumentom inštitúcií, orgánov, úradov a agentúr Únie a požiadavky týchto inštitúcií, orgánov, úradov a agentúr Únie na zabezpečenie transparentnosti ich konania.

1.2. Charta základných práv EU

Transparentnosť je dôležitým prvkom zásady spravodlivého spracovania. Takáto transparentnosť je zahrnutá v článku 8 Charty základných práv EÚ.

Článok 8

Ochrana osobných údajov

1. Každý má právo na ochranu osobných údajov, ktoré sa ho týkajú.

2. Tieto údaje musia byť riadne spracované na určené účely na základe súhlasu dotknutej osoby alebo na inom oprávnenom základe ustanovenom zákonom. Každý má právo na prístup k zhromaž deným údajom, ktoré sa ho týkajú, a právo na ich opravu.

3. Dodržiavanie týchto pravidiel podlieha kontrole nezávislého orgánu.

1.3. GDPR

Recitál 39

Každé spracúvanie osobných údajov by malo byť zákonné a spravodlivé. Pre fyzické osoby by malo byť transparentné, že sa získavajú, používajú, konzultujú alebo inak spracúvajú osobné údaje, ktoré sa ich týkajú, ako aj to, v akom rozsahu sa tieto osobné údaje spracúvajú alebo budú spracúvať. Zásada transparentnosti si vyžaduje, aby všetky informácie a komunikácia súvisiace so spracúvaním týchto osobných údajov boli ľahko prístupné a ľahko pochopiteľné a formulované jasne a jednoducho. Uvedená zásada sa týka najmä informácií pre dotknuté osoby o identite

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

prevádzkovateľa a účeloch spracúvania, a ďalších informácií na zabezpečenie spravodlivého a transparentného spracúvania, pokiaľ ide o dotknuté fyzické osoby a ich právo získať potvrdenie a oznámenie spracúvaných osobných údajov, ktoré sa ich týkajú. Fyzické osoby by mali byť upozornené na riziká, pravidlá, záruky a práva pri spracúvaní osobných údajov, ako aj na to, ako uplatňovať svoje práva pri takomto spracúvaní. Najmä konkrétne účely, na ktoré sa osobné údaje spracúvajú, by mali byť výslovne uvedené a legitímne a stanovené v čase získavania osobných údajov. Osobné údaje by mali byť primerané, relevantné a obmedzené na rozsah, ktorý je nevyhnutný vzhľadom na účely, na ktoré sa spracúvajú. To si vyžaduje najmä zabezpečenie toho, aby obdobie, počas ktorého sa tieto osobné údaje uchovávajú, bolo obmedzené na nevyhnutný rozsah. Osobné údaje by sa mali spracúvať len vtedy, ak účel spracúvania nebolo možné za primeraných podmienok dosiahnuť inými prostriedkami. S cieľom zabezpečiť, aby sa osobné údaje neuchovávali dlhšie, než je to nevyhnutné, by mal prevádzkovateľ stanoviť lehoty na vymazanie alebo pravidelné preskúmanie. Mali by sa prijať všetky primerané opatrenia, aby sa zabezpečila oprava alebo vymazanie nesprávnych údajov. Osobné údaje by sa mali spracúvať tak, aby sa zabezpečila primeraná bezpečnosť a dôvernosť osobných údajov vrátane predchádzania neoprávnenému prístupu k osobným údajom a zariadeniu používanému na spracúvanie, alebo neoprávnenému využitiu týchto údajov a zariadení.

Recitál 58

Zásada transparentnosti si vyžaduje, aby všetky informácie určené verejnosti alebo dotknutej osobe boli stručné, ľahko prístupné a ľahko pochopiteľné, formulované jasne a jednoducho, a navyše ak je to vhodné, ľahko zrakovo vnímateľné. Takéto informácie by sa mohli poskytnúť v elektronickej podobe, napríklad pri oslovení verejnosti prostredníctvom webového sídla. Týka sa to najmä situácií, ako je napríklad online reklama, v ktorých veľký počet účastníkov a technologická zložitosť činnosti sťažujú dotknutej osobe zistiť a pochopiť, či osobné údaje, ktoré sa jej týkajú, boli získané, kým a na aké účely. Keďže deťom prislúcha osobitná ochrana, všetky informácie a každá komunikácia, pri ktorej sa spracúvanie zameriava na dieťa, by mali byť formulované jasne a jednoducho, aby ich dieťa mohlo ľahko pochopiť.

Článok 5, odsek 1

Zásady spracúvania osobných údajov

1. *Osobné údaje musia byť:*

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

(a) spracúvané zákonným spôsobom, spravodlivo a transparentne vo vzťahu k dotknutej osobe („zákonnosť, spravodlivosť a transparentnosť“);

2. VÝZNAM TRANSPARENTNOSTI PODĽA GDPR

Princíp transparentnosti je spojený so zásadami spravodlivosti a zodpovednosti. Článok 5 (Zásady týkajúce sa spracovania osobných údajov) ukladá kontrolórom povinnosť preukázať, že osobné údaje sú spracovávané transparentným spôsobom. Podľa pracovnej skupiny[i], podľa Článku 29 o ochrane údajov je transparentnosť zameraná na to, aby dotknutým osobám bolo umožnené, aby sa kontrolóri údajov a spracovatelia zodpovedali a aby vykonávali kontrolu nad ich osobnými údajmi[ii]. Tento cieľ sa realizuje zavedením špecifických praktických požiadaviek, ktoré by sa mali dodržiavať vo všetkých fázach spracovania.

2.1. Súčasti transparentnosti v zmysle GDPR (Čl. 12)

2.1.1. “Stručné, prehľadné, zrozumiteľné a ľahko dostupné”

Prvé dve časti tejto požiadavky znamenajú, že kontrolóri údajov by mali účinne a stručne uvádzať informácie / komunikáciu, aby sa predišlo informačnej preťaženosti (alebo inak povedané, aby boli dotknuté osoby informované). Spôsob, ako tak urobiť, je formou vrstevných oznámení, kde sú dotknuté osoby informované o svojich právach postupne (napríklad poskytnutie kľúčových informácií v krátkom čase a zvyšok - v čase zhromažďovania údajov). Tieto informácie by mali byť oddelené od iných informácií, ktoré sa netýkajú súkromia, ako sú zmluvné ustanovenia.

Požiadavka, aby informácia bola "zrozumiteľná", znamená, že by jej mal rozumieť priemerný člen cieľového publika, v tomto prípade priemerného občana miestnej komunity. Dotknuté osoby by mali byť schopné vopred určiť, aký rozsah a dôsledky spracovania je obsiahnuty. Článok 29 Pracovná skupina (WP29) odporúča, aby kontrolóri údajov jednoznačne vysvetlili, aké budú najdôležitejšie dôsledky spracovania, najmä ak tieto dôsledky môžu mať vplyv na základné práva dotknutých osôb[iii].

"Ľahko prístupný" element znamená, že dotknutá osoba by nemala hľadať informácie. Namiesto toho by mal byť prezentovaný jasným spôsobom, takže sa k nemu môže bez ťažkostí dostať.

2.1.2. “Jasný a jednoduchý jazyk“

Požiadavka na jasný a jednoduchý jazyk znamená, že informácie by sa mali poskytovať čo najjednoduchším spôsobom a vyhnúť sa zložitým vetným a jazykovým štruktúram. Informácie by nemali byť formulované v abstraktných alebo ambivalentných pojmoch

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

terminology[iv], ani by nemali priestor na rôzne interpretácie. Účely a právny základ spracovania osobných údajov by mali byť jasné. Musí sa zabrániť akejkoľvek nejasnej formulácii účelov spracovania, ako je "pre rozvoj budúcich služieb" "na výskumné účely". Informácie poskytované dotknutej osobe by nemali obsahovať príliš legalizačný, technický alebo špecializovaný jazyk alebo terminológiu[v].
Miestne orgány by mali tiež zabezpečiť, aby slovná zásoba, tón a štýl jazyka, ktorý sa používa pri oslovovaní detí, boli primerané a rezonujú s deťmi, aby si uvedomili, že ich správa / informácie smerujú k nim[vi].

2.1.3. Spôsob poskytovania informácií (Čl. 12, ods.1 a ods 5 “bez poplatku”).

Správcovia údajov nemôžu účtovať dotknutej osobe za poskytovanie informácií podľa článkov 13 a 14 (informácie, ktoré sa majú poskytnúť dotknutej osobe) alebo za oznámenia a opatrenia prijaté podľa článkov 15 - 22 (práva dotknutých osôb) a článku 34 (oznámenie porušenia osobných údajov dotknutých osôb). Existuje jedna výnimka z tohto pravidla: ak sú žiadosti od dotknutej osoby zjavne neodôvodnené, alebo neprimerané, najmä z dôvodu ich opakujúceho sa charakteru. V tomto prípade môže prevádzkovateľ účtovať primeraný poplatok, pričom zohľadní administratívne náklady na poskytovanie informácií alebo komunikáciu alebo na vykonanie požadovanej činnosti. Pre správcov údajov je dôležité vedieť, že znášajú bremeno preukázania zjavne neopodstatneného alebo neprimeraného charakteru žiadosti. Z tohto dôvodu nie je vhodné, aby miestne orgány účtovali za poskytovanie informácií podľa GDPR občanom.

2.2. Informácie poskytované dotknutým osobám (Čl.13 a Čl.14)

2.2.1. Aké informácie poskytnúť?

Články 13 a 14 GDPR stanovujú, ktoré informácie musia byť dotknutej osobe poskytnuté. V nariadení sa rozlišuje medzi prípadmi, keď informácie poskytla dotknutá osoba (článok 13) a kedy nebol (článok 14). Miestne orgány by mali poskytnúť:

1) informácie o ich totožnosti vrátane ich kontaktných informácií;
2) kontaktné údaje úradníka pre ochranu údajov;
3) účely spracovania a ich právneho založenia - prevažne pre miestne orgány nadáciou by bol článok 6 ods. 1 písm. e) výkon úradnej právomoci, ktorú má kontrolór, a príslušné ustanovenia právnych predpisov členského štátu;
4) typ údajov, ktoré sa spracúvajú, v prípade ak ich dotknutá osoba neposkytla;
5) totožnosť možných príjemcov údajov - nielen tretie strany, ale aj spracovatelia a spoloční kontrolóri. Kontrolór by mal byť pri definovaní rôznych kategórií príjemcov údajov čo najkonkrétnejší.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

2.2.2 Aké dodatočné informácie poskytnúť?

Po prvé, na zabezpečenie spravodlivého a transparentného spracovania musí prevádzkovateľ poskytnúť dotknutej osobe:

1) obdobie, počas ktorého sa osobné údaje budú uchovávať, alebo kritériá použité na určenie tohto obdobia;
2) existencia práva požiadať prevádzkovateľa o prístup k údajom alebo o opravu alebo vymazanie osobných údajov alebo obmedzenie spracovania údajov, ktoré sa týkajú dotknutej osoby, alebo namietať proti spracovaniu, ako aj práva na prenos údajov;
3) ak je spracovanie založené na súhlase, existencia práva na odstúpenie od zmluvy vyžaduje udeliť súhlas kedykoľvek;
4) právo podať sťažnosť orgánu pre dohľad;
5) existencia automatizovaného rozhodovania vrátane profilovania a zmysluplné informácie o príslušnej logike, ako aj význam a predpokladané následky takéhoto spracovania pre dotknutú osobu.

Informácie o profilovaní by mali byť nielen ľahko dostupné pre dotknuté osoby, ale musia byť im upozornené. Riadiaci pracovník by mal nájsť jednoduché spôsoby, ako povedať dotknutej osobe o logike alebo kritériách použitých na automatizované rozhodovanie bez zrozumiteľných vysvetlení algoritmov.

Ak údaje neboli získané od dotknutej osoby, kontrolór údajov by mal poskytnúť svoj zdroj. Ak dotknutáj osoba poskytuje údaje, kontrolór by mal informovať ho, ak je poskytovanie osobných údajov zákonnou požiadavkou.

Po druhé, kontrolóri by mali informovať dotknuté osoby, ak majú v úmysle spracúvať údaje na akékoľvek účely odlišné od tých, na ktoré boli údaje zhromaždené. Dotknutým osobám sa musia poskytnúť informácie o tomto inom účelu a o všetkých ďalších relevantných informáciách, ktoré sú totožné s informáciami poskytnutými na pôvodný účel (obdobie spracovania, právny základ spracovania atď.). Pri získavaní údajov by mohlo byť užitočné informovať dotknuté osoby o prípadnom budúcom spracovaní, ak je pravdepodobné, že sa uskutočnia vzhľadom na činnosť kontrolóra.

2.2.3 Ako majú byť informácie poskytnuté?

Štandardný spôsob poskytovania informácií a komunikácie s dotknutými osobami subject je písomný. GDPR však umožňuje aj poskytovanie informácií inými prostriedkami, vrátane elektronických. Podľa WP29 je rozhodujúce, aby zvolené metódy poskytovania informácií boli vhodné pre konkrétne situácie[vii]. Informácie môžu byť sprístupnené na požiadanie ústne dotknutej osobe, ak sú ich informácie o totožnosti preukázané inými (t. j. neverbálnymi) prostriedkami. Existuje výnimka z tohto pravidla, týkajúca sa informácií,

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

ktoré by mali prevádzkovatelia údajov poskytnúť podľa čl. 13 a 14 - táto informácia môže byť predmetnej osobe odhalená bez kontroly totožnosti. Ústne poskytovanie informácií nemusí nevyhnutne znamenať ústne informácie poskytnuté osobne, mohlo by to znamenať automatizované ústne informácie. Podľa WP29 by mal správca údajov umožniť dotknutej osobe opätovne počúvať predtým zaznamenané správy, najmä ak ide o zrakovo postihnuté osoby alebo iné dotknuté osoby, ktoré môžu mať ťažkosti s prístupom alebo porozumením informácií v písomnej podobe. Aj v prípadoch ústneho poskytovania informácií by správcovia údajov mali byť stále schopní preukázať, že spĺňajú požiadavky GDPR. Aby tak urobili, mali by zabezpečiť, aby mali záznam o 1) žiadosti o informácie prostredníctvom ústnych prostriedkov, 2) spôsob, akým bola totožnosť dotknutej osoby overená a 3) skutočnosť, že informácie boli poskytnuté subjektívne[viii].

2.2.4. Kedy poskytnúť informácie?

Informácie o spracovaní osobných údajov sa dotknutej osobe poskytnú v čase zberu údajov (článok 13 ods. 1). Ak údaje nie sú získané priamo od dotknutej osoby, ale z iného zdroja, informácie sa poskytnú dotknutej osobe v primeranej lehote, najneskôr však do jedného mesiaca od získania, v závislosti od okolností daného prípadu. Existujú dva špecifické prípady: po prvé, ak sa údaje používajú na komunikáciu s predmetom, informácie by mali byť poskytnuté najneskôr v čase prvého oznámenia dotknutej osobe údajov; a po druhé, ak sa očakáva, že údaje budú zverejnené inému príjemcovi, najneskôr pri prvom zverejnení tomuto príjemcovi.
Táto lehota môže byť predĺžená na maximálne tri mesiace z dôvodu zložitosti a počtu žiadostí (napríklad ak žiadosť zahŕňa viac databáz). Kontrolór musí informovať dotknutú osobu o každom takomto predĺžení do jedného mesiaca od prijatia žiadosti spolu s dôvodmi na oneskorenie a informáciami o právach dotknutej osobey podať sťažnosť.

2.2.5. Kedy upozorniť na zmeny transparentnosti informácií, ktoré by mali byť poskytnuté kontrolórmi údajov?

V situácii, kedy by zmena informácií mohla mať vážny dopad na dotknutú osobu, správcovia údajov by mali poskytnúť informácie v dostatočnom predstihu pred tým, ako zmena skutočne nadobudne účinnosť [ix]. Toto by sa malo robiť jasným a účinným spôsobom. Občania by mali mať dostatok času na to, aby zvážili povahu a vplyv zmeny a uplatňovali svoje práva v rámci GDPR vo vzťahu k zmene, napríklad aby vznášali námietky proti spracovaniu. WP29 odporúča, aby pravidelne basis[x] obnovovali práva dotknutej osoby v oblasti spracovania údajov[xi].
Ak plánujete spracovávať údaje na iný účel ako tie, na ktoré boli získané, dotknuté osoby by mali byť informované pred začatím nového spracovania údajov.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

2.3. Metódy

Spôsoby sú formáty, v ktorých prevádzkovatelia údajov plnia svoju povinnosť v rámci GDPR poskytovať informácie dotknutým osobám.

2.3.1. Upozornenia o ochrane osobných údajov

Pokiaľ ide o on-line platformy, je potrebné používať vrstvené vyhlásenia o ochrane osobných údajov / upozornenia na prepojenie na rôzne kategórie informácií, ktoré sa musia poskytnúť dotknutej osobe namiesto použitia jediného oznámenia[xii]. Tento prístup umožňuje používateľom navigovať priamo do časti oznámenia, ktorú si želajú prečítať. Pri vytváraní takéhoto vrstveného upozornenia sa musia kontrolóri snažiť poskytnúť jasný a zrozumiteľný prehľad (alebo obsah), takže dotknuté osoby si uvedomujú, kde môžu nájsť jednotlivé informácie.

2.3.2. “Push” & “pull” notices

Článok 29 Pracovná skupina tiež zavádza používanie oznámení "push" a "pull". Hlavný rozdiel spočíva v tom, že v druhom prípade sa od používateľov webových stránok očakáva, že budú požadovať informácie, v tomto prípade informácie o spracovaní ich údajov, zatiaľ čo v prvom prípade je oznámenie "tlačené" na obrazovku bez akejkoľvek activity z ich strany. WP29 uvádza príklady a definície tlačových oznámení s upozorneniami transparentnosti "just-in-time" a pre upozornenia "pull" - s prehľadnými panelmi a návodmi na získanie informácií[xiii]:

- *Oznámenie "just-in-time"* sa používa na poskytovanie špecifických "informácií o ochrane osobných údajov", ak sa to pre dotknutú osobu považuje za najrelevantnejšie. Tento formát môže byť užitočný, ak webová lokalita miestneho úradu zabezpečí vykonanie určitej služby online po vyplnení formulára. Predtým, než občan vyplní formulár, môže sa objaviť takéto upozornenie.
- *Dashboard pre transparentnosť* je jednoduchý bod, od ktorého môžu dotknuté osoby zobrazovať "informácie o ochrane osobných údajov" a spravovať svoje preferencie ochrany osobných údajov tým, že umožnia, alebo zabránia tomu, aby sa ich údaje používali určitými spôsobmi.

2.3.3. Iné typy “vhodných opatrení “

Mimo digitálneho prostredia podľa WP29 säú vhodné opatrenia aj tieto:

- Tlačená a papierová oblasť: písomné vysvetlenia, letáky;
- Telefonická oblasť: ústne vysvetlenia reálnej osoby, automatizované alebo vopred zaznamenané informácie s možnosťou vypočutia podrobnejších informácií;

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

- QR kódy, hlasové upozornenia, písomné informácie o inteligentnom zariadení, správy zasielané SMS alebo e-mailom a iné;
- Životné prostredie človeka: ústne vysvetlenia, písomné vysvetlenia poskytnuté v pevnom alebo mäkkom formáte [xiv].

2.3.4. Vizualizácia

GDPR zavádza vizualizačné nástroje (odkazujúce najmä na ikony, certifikačné mechanizmy a pečate a ochranné známky ochrany údajov). Zmyslom použitia ikon je poskytnúť informácie dotknutým osobám prístupným spôsobom pomocou štandardizovaných symbolov / obrazov, ktoré sú uznávané v celej EÚ. Vývoj "kódu ikon" ešte nezačal. V GDPR sa tiež ustanovuje používanie mechanizmov na udeľovanie osvedčení o ochrane údajov, pečatí na ochranu údajov a značiek na účely preukázania súladu s nariadením. Členské štáty, orgány pre dohľad, európsky orgán na ochranu údajov alebo Komisia stanovili certifikačné mechanizmy, ktoré preukážu, že prevádzkovateľ dodržiava GDPR a dokazuje, že dodržiava technické a organizačné opatrenia na splnenie noriem na ochranu údajov. Tieto formáty sa môžu uplatniť v subjektoch, ktoré nie sú verejnými orgánmi, ako napríklad autonómna obecná spoločnosť.

2.4. Výkonnosť práv dotknutých osôb

Dotknuté osoby majú právo získať od správcov údajov informácie týkajúce sa ich osobných údajov. Informácie, ktoré musia byť poskytnuté v rámci GDPR, sú výslovne uvedené v čl. 13 a čl. 14 a dotknuté osoby nemusia podávať žiadnu žiadosť alebo podniknúť žiadne iné aktívne kroky na ich získanie, na rozdiel od toho, keď vykonávajú svoje iné práva (právo na prístup, opravu, vymazanie atď.).

2.4.1. Výnimky z povinnosti poskytovať právo na informácie

Právo na informácie nie je absolútne, inými slovami je obmedzené v určitých situáciách. V niektorých prípadoch sú miestne orgány oslobodené od povinnosti poskytnúť vyššie uvedené informácie. Ak sú údaje získané od dotknutej osoby, jediný taký prípad je, keď už má dané informácie (článok 13 ods. 4).

Ak údaje nie sú získané od dotknutej osoby, výnimiek je viac (článok 14 ods. 5):

- keď dotknutá osoba už má informácie;
- keď sa ukáže, že poskytnutie takýchto informácií je nemožné, by to viedlo k neprimeranému úsiliu alebo k nemožnému alebo vážnemu narušeniu dosiahnutia cieľov spracovania; príkladom nemožnosti poskytnúť informácie by bolo, keby kontrolór nemal žiadne prostriedky na kontaktovanie dotknutej osoby;
- ak je získanie alebo zverejnenie výslovne ustanovené v právnych predpisoch EÚ

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

alebo členských štátov EÚ, čo je najbežnejšia hypotéza pre miestne orgány;

- keď sa na osobné údaje vzťahuje povinnosť zachovávať služobné tajomstvo, ktorú upravuje právo Únie alebo členského štátu vrátane zákonnej povinnosti mlčanlivosti; táto výnimka sa môže uplatniť na autonómne obecné spoločnosti a podobné subjekty.

Podľa WP29[xv], by sa tieto výnimky mali vo všeobecnosti interpretovať a uplatňovať čo najpresnejšie.

3. ZÁVER A PRAKTICKÉ RADY

Princíp transparentnosti je jedným zo základov GDPR. V mnohých ohľadoch zabezpečuje, aby fyzické osoby mali k dispozícii všetky informácie, ktoré potrebujú na to, aby boli oboznámení s tým, aké osobné údaje sa o nich spracúvajú a ktoré slúžia na výkon ich práv podľa Nariadenia. Informácie by mali byť ľahko prístupné a ľahko pochopiteľné jasným a jednoduchým jazykom.

Orgánom miestnej samosprávy sa odporúča, aby vytvorili zoznam všetkých informácií požadovaných v GDPR a aby si vybrali tie najlepšie spôsoby, ako osloviť občanov, ktorých údaje spracovávajú. Napríklad môžu uviesť informačné listy vo verejných kanceláriách a poskytnúť letáky obsahujúce informácie podľa článku 13 a čl. 14 a rozdeľte ich. Elektronické prostriedky môžu byť užitočné napríklad vtedy, keď daná entita využíva on-line platformu / platformu, ale v určitých prípadoch môžu byť potrebné aj tlačené formáty. Osobitná pozornosť by sa mala venovať tomu, že webové portály MO ponúkajú online služby. Treba tiež mať na pamäti, že niektoré autonómne komunálne spoločnosti (napríklad spoločnosti verejnej dopravy) vykonávajú viac druhov spracovania a disponujú obrovskými databázami, a preto by mali vynaložiť viac úsilia na zostavenie informácií podľa čl. 13 a 14.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

4. EXTERNÉ ZDROJE a WEBLINKy

Bibliografia

- **Voigt, P., von dem Bussche, A.**, The EU General Data Protection Regulation (GDPR) – A Practical Guide, Springer International Publishing (2017);
- Bird & Bird Guide to General Data Protection Regulation (2016);
- EU General Data Protection Regulation (GDPR). An Implementation and Compliance Guide, IT Governance Publishing, Cambridgeshire (2016);

Dokumenty Článku 29 - Pracovná časť

- Article 29 Data Protection Working Party, Guidelines on transparency under Regulation 2016/679, WP260;

Webové Linky

- http://europa.eu/rapid/press-release_IP-18-386_en.htm
- https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en

5. REFERENCES

[i] The Article 29 Working Party (WP) is established on the basis of Art. 29 of Directive 95/46/EC, which will be replaced by the GDPR. The goal of the WP is to provide opinions and recommendations and to advice on personal data protection.
[ii] Article 29 Data Protection Working Party, Guidelines on transparency under Regulation 2016/679, p. 23
[iii] Ibid, p. 8
[iv] Ibid, p. 9
[v] Ibid
[vi] Ibid
[vii] Ibid, p. 21
[viii] Ibid, p. 12
[ix] Ibid, p. 15
[x] Ibid, p. 16
[xi] Ibid, p. 16
[xii] Ibid, p. 17
[xiii] Ibid, p. 17-18
[xiv] Ibid, p. 18-19
[xv] Ibid, p. 25

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

ProLegis

Zverejňovanie informácií alebo právo na prístup dotknutej osoby Článok 15 GDPR

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

Contents

1. Legal framework 3
   1.1. General Data Protection Regulation (GDPR) 3
2. Basics 5
3. Details of disclosing information to the data subject 5
   3.1. Substance of disclosure 5
   3.2. How much time has the controller to answer (deadline)? 6
   3.3. In what form can be claimed and how should it be answered? 7
   3.4. Has the applicant's identity as the data subject to be proven? 8
   3.5. Costs? May the information be reimbursed? 8
   3.6. Is there an obligation for the applicant to participate in the disclosure? 8
   3.7. Do the rights of third parties have to be taken into account when providing information? 9
4. Checklist for disclosing information on request 10
   4.1. Issuing the information 11
5. External Sources & WEBLINKS 12
   5.1. Books and Articles 12
   5.2. Other Documents and cases 12

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

1. Právny rámec

1.1. General Data Protection Regulation (GDPR)

Článok 15

Právo dotknutej osoby na prístup k údajom

1. Dotknutá osoba má právo získať od prevádzkovateľa potvrdenie o tom, či sa spracúvajú osobné údaje, ktoré sa jej týkajú, a ak tomu tak je, má právo získať prístup k týmto osobným údajom a tieto informácie:

(a) účely spracúvania;

(b) kategórie dotknutých osobných údajov;

(c) príjemcovia alebo kategórie príjemcov, ktorým boli alebo budú osobné údaje poskytnuté, najmä príjemcovia v tretích krajinách alebo medzinárodné organizácie;

(d) ak je to možné, predpokladaná doba uchovávania osobných údajov alebo, ak to nie je možné, kritériá na jej určenie;

(e) existencia práva požadovať od prevádzkovateľa opravu osobných údajov týkajúcich sa dotknutej osoby alebo ich vymazanie alebo obmedzenie spracúvania, alebo práva namietať proti takémuto spracúvaniu;

(f) právo podať sťažnosť dozornému orgánu;

(g) ak sa osobné údaje nezískali od dotknutej osoby, akékoľvek dostupné informácie, pokiaľ ide o ich zdroj;

(h) existencia automatizovaného rozhodovania vrátane profilovania uvedeného v článku 22 ods. 1 a 4 a v týchto prípadoch aspoň zmysluplné informácie o použitom postupe, ako aj význame a predpokladaných dôsledkoch takéhoto spracúvania pre dotknutú osobu.

2. Ak sa osobné údaje prenášajú do tretej krajiny alebo medzinárodnej organizácii, dotknutá osoba má právo byť informovaná o primeraných zárukách podľa článku 46 týkajúcich sa prenosu.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

3. Prevádzkovateľ poskytne kópiu osobných údajov, ktoré sa spracúvajú. Za akékoľvek ďalšie kópie, o ktoré dotknutá osoba požiada, môže prevádzkovateľ účtovať primeraný poplatok zodpovedajúci administratívnym nákladom. Ak dotknutá osoba podala žiadosť elektronickými prostriedkami, informácie sa poskytnú v bežne používanej elektronickej podobe, pokiaľ dotknutá osoba nepožiadala o iný spôsob.

4. Právo získať kópiu uvedenú v odseku 3 nesmie mať nepriaznivé dôsledky na práva a slobody iných.

Recitály 63 a 64:

(63) Dotknutá osoba by mala mať právo na prístup k osobným údajom, ktoré boli o nej získané, a uvedené právo aj jednoducho a v primeraných intervaloch uplatňovať, aby si bola vedomá zákonnosti spracúvania a mohla si ju overiť. K tomu patrí aj právo dotknutých osôb na prístup k údajom týkajúcim sa ich zdravia, napríklad k údajom v ich lekárskych záznamoch obsahujúcich informácie ako diagnóza, výsledky vyšetrení, posudky ošetrujúcich lekárov a akákoľvek poskytnutá terapia alebo uskutočnené zákroky. Každá dotknutá osoba by preto mala mať právo vedieť a byť informovaná najmä o účeloch spracúvania osobných údajov, podľa možnosti o dobe spracúvania osobných údajov, o príjemcoch osobných údajov, o postupe v každom automatickom spracúvaní osobných údajov a aspoň v prípadoch, v ktorých sa spracúvanie opiera o profilovanie, o následkoch takéhoto spracúvania. Ak je to možné, prevádzkovateľ by mal môcť poskytnúť prístup na diaľku k bezpečnému systému, ktorý by dotknutej osobe zabezpečil priamy prístup k jej osobným údajom. Uvedené právo by sa nemalo nepriaznivo dotknúť práv alebo slobôd iných osôb, ani obchodného tajomstva alebo práv duševného vlastníctva a najmä autorských práv týkajúcich sa softvéru. Výsledkom zohľadnenia týchto prvkov by však nemalo byť odmietnutie poskytnutia akýchkoľvek informácií dotknutej osobe. Ak prevádzkovateľ spracúva v súvislosti s dotknutou osobou veľké množstvo informácií, mal by môcť požadovať, aby pred doručením informácií dotknutá osoba spresnila, ktorých informácií alebo spracovateľských činností sa žiadosť týka.

(64) Prevádzkovateľ by mal použiť všetky primerané opatrenia na overenie totožnosti dotknutej osoby, ktorá žiada o prístup k údajom, najmä v súvislosti s online službami a online identifikátormi. Prevádzkovateľ by nemal uchovávať osobné údaje len preto, aby bol schopný reagovať na prípadné žiadosti

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

2. Základné informácie

GDPR ustanovuje v článku 15 právo zverejniť všetky informácie, ktoré má dotknutá osoba k dispozícii na základe svojej žiadosti (napr. Zákazník, zamestnanec, uchádzač o zamestnanie, pacient, ďalej len "subjekt údajov") vo vzťahu k (napr. spoločnosť, zamestnávateľ, prevádzkovateľ nemocnice). Toto sa nazýva "Právo na prístup dotknutej osoby (k jej údajom). Účelom tohto práva je, aby dotknutá osoba mohla získať informácie o obsahu a podrobnostiach o údajoch, ktoré sa o nej spracovávajú, s cieľom prípadného uplatnenia ďalších práv dotknutých osôb (napr. Oprava alebo vymazanie podľa článku 16 GDPR) alebo zákonnosť spracovania.

Toto právo je ústrednou inštitúciou zákona o ochrane údajov, pretože sa často považuje za základ pre dotknutú osobu na uplatnenie akýchkoľvek iných práv. Napriek tomu, že orgány na ochranu údajov (DPA) v rámci GDPR majú právomoc kontrolovať kontrolóra bez konkrétneho podnetu na sťažnosť, v praxi (z dôvodu obmedzených zdrojov orgánov na ochranu údajov) je zvyčajne neúplné alebo oneskorené zverejnenie v zmysle práva osôb na prístup k údajom, DPA k plánu. Práve na tento účel by mali byť kontrolóri dobre pripravení.

Najlepšou prípravou sú dobre štruktúrované a najpodrobnejšie záznamy o spracovateľských činnostiach. Čím lepšie je táto dokumentácia sformovaná spolu s obchodnými procesmi, pre ktoré sú spracúvané osobné údaje, tým ľahšie bude možné nájsť konkrétne údaje špecifického predmetu v rámci žiadostí a v primeranom čase.

3. Podrobnosti o zverejňovaní údajov dotknutej osoby

3.1. Podstata zverejnenia

Právo na prístup oprávňuje dotknutú osobu na:

i. Právo požiadať kontrolóra, aby potvrdil, či sa jeho osoba spracúva resp. nespracúva; ak je to potrebné, na otázku by mala byť odpoveď "negatívna", ak nie sú spracované žiadne údaje o tejto osobe (tzv. "negatívne informácie"): "*Nespracujeme údaje o vás*";

ii. Právo na získanie kópie osobných údajov, ktoré sú predmetom spracovania (akékoľvek dodatočné kópie vyžiadané subjektom údajov, za ne môže prevádzkovateľ účtovať primeraný poplatok na základe administratívnych nákladov.) Ak dotknutá osoba podá žiadosť elektronicky, potom informácie sa poskytnú v spoločnom elektronickom formáte, ak nie je uvedené inak.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

iii. Právo na získanie nasledovných informácií:

Čl. 15 Par. 1 GDPR	Obsah infromácie
písmneno a	Účel spracovania
písmneno b	kategórie dotknutých osobných údajov
písmneno c	**príjemcovia alebo kategórie príjemcov**, ktorým boli alebo budú osobné údaje poskytnuté, najmä príjemcovia v tretích krajinách alebo medzinárodné organizácie
písmeno d	ak je to možné, **predpokladaná doba uchovávania osobných údajov budú uchovávať**, alebo ak to nie je možné, kritériá použité na určenie tohto obdobia;
písmneno e	**existencia práva požadovať od prevádzkovateľa opravu osobných údajov týkajúcich sa dotknutej osoby alebo ich vymazanie alebo obmedzenie** spracúvania, alebo práva namietať proti takémuto spracúvaniu;
písmneno f	**právo podať sťažnosť** dozornému orgánu
písmneno g	ak sa osobné údaje nezískali od dotknutej osoby**, akékoľvek dostupné informácie, pokiaľ ide o ich zdroj**
písmneno h	existencia **automatizovaného rozhodovania vrátane profilovania** uvedeného v článku 22 ods. 1 a 4 a v týchto prípadoch aspoň zmysluplné informácie o použitom postupe, ako aj význame a predpokladaných dôsledkoch takéhoto spracúvania pre dotknutú osobu.
Para 2	Ak sa osobné údaje **prenášajú do tretej krajiny alebo medzinárodnej** organizácii, dotknutá osoba má právo byť informovaná o primeraných zárukách podľa článku 46 týkajúcich sa prenosu.

Poznámka: Podľa článku 23 by **právo na informácie mohlo byť obmedzené vnútroštátnymi právnymi predpismi.**

3.2. Koľko času má kontrolór na odpoveď (termín)?

V zásade musí byť žiadosť o informácie zodpovedaná promptne, najneskôr však do jedného mesiaca od prijatia žiadosti (článok 12 ods. 3) GDPR). Toto obdobie sa môže predĺžiť o ďalšie dva mesiace, ak je to potrebné, s prihliadnutím na zložitosť a počet žiadostí. Kontrolór informuje dotknutú osobu o predĺžení termínu do jedného mesiaca od doručenia žiadosti spolu s dôvodmi oneskorenia. Ak príslušná osoba predloží žiadosť elektronicky, dotknutá osoba je podľa možnosti informovaná elektronicky, ak nie je uvedené inak.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

Ak prevádzkovateľ nereaguje na žiadosť dotknutej osoby, bezodkladne informuje dotknutú osobu, najneskôr však do jedného mesiaca od doručenia žiadosti, o dôvodoch a o možnosti podať sťažnosť orgánu dozoru alebo podať opravný prostriedok.

3.3. V akej forme sa môže uplatniť nárok a akým spôsobom odpoveda?

Neexistuje žiadny nátlak na spôsob, žiadosť o informácie môže byť podaná ústne, písomne alebo v digitálnej podobe (napríklad prostredníctvom e-mailu). Odpoveď na žiadosť o informácie sa môže uskutočniť v akejkoľvek vhodnej forme, ale je potrebné poznamenať:

- Písomnej žiadosti sa volí písomná forma odpovede. Jednou z bežných metód bola v minulostitá, keď odporca predložil kópiu preukazu totožnosti (úradné číslo) na svoju žiadosť a zodpovedná osoba odpovedala ako na doporučenú poštu (s výnimkou zástupcov dodávateľov). Vzhľadom na to, že úradné identifikačné číslo zvyčajne obsahuje väčšie množstvo údajov potrebných na identifikáciu dotknutých osôb, odporúča sa písomne predložiť iba informácie o názve, osobnom identifikačnom čísle a / alebo sériovom čísle dokladu totožnosti dotknutou osobou.
- Ak to žiadateľ požaduje, informácie sa môžu poskytnúť ústne za predpokladu, že totožnosť dotknutých osôb bola stanovená v inej forme.
- Ak dotknutá osoba predloží žiadosť elektronicky (napr. Elektronickou poštou), informácie sa poskytnú v spoločnom elektronickom formáte, pokiaľ nie je uvedené inak. Ak je to možné, môže riadiaci orgán poskytovať aj externý prístup k zabezpečenému systému, ktorý poskytne dotknutej osobe priamy prístup k svojim osobným informáciám.

Upozornenie! Všetky oznámenia musia byť poskytnuté v **jasnom a jednoduchom jazyku** v presnej, transparentnej, zrozumiteľnej a ľahko prístupnej forme (to platí najmä pre informácie, ktoré sú zamerané konkrétne na deti). Rovnako ako v minulosti musia byť skratky obsiahnuté v odpovedi vysvetlené správcom v jeho odpovedi.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

3.4. *Preukazuje as totožnosť žiadateľa ako dotknutej osoby?*

Áno. Identita osoby, ktorá požaduje informácie (dotknutá osoba) musí byť jednoznačná, pretože prevádzkovateľ môže požiadať o dodatočné informácie, ak má "odôvodnenú pochybnosť" o totožnosti fyzickej osoby, ktorá podáva žiadosť (pozri článok 12 odsek 6[1]).

Podľa odôvodnenia 64 by kontrolór mal používať všetky primerané prostriedky na overenie totožnosti subjektu údajov, ktorý sa snaží získať informácie, najmä v súvislosti s službami online a v prípade on-line identifikátorov.

Autentifikácia totožnosti by sa mala navrhnúť tak, aby spĺňala povinnosť zabezpečiť bezpečnosť údajov v súlade s rizikom, inak by mohlo dôjsť k narušeniu údajov, ak sa dáta prenášajú nesprávnemu príjemcovi.

Bežnou praxou v Rakúsku podľa predchádzajúceho zákona o ochrane údajov (DSG 2000) bolo, že žiadateľ predložil svoju prihlášku a kópiu identifikačného dokumentu (úradného dokladu) a správca poskytol odpoveď na pošte ako "osobný" doporučený list (okrem oprávnených zástupcov). Totožnosť však môže vyplývať jednoznačne aj zo situácie, napr. ak existuje neustály kontakt s poskytovateľom informácií a toto (a jeho adresa) je preto známe[2].

3.5. *Náklady? Môžu byť hradené?*

V zásade sa informácie musia poskytovať bezplatne (pozri článok 12 ods. 5 GDPR). Avšak v prípade zjavne neopodstatnených alebo najmä v prípade častého opakovania nadmerných požiadaviek subjektu údajov môže správca buď:

(a) vyžadovať primeraný poplatok, berúc do úvahy administratívne náklady na oznamovanie alebo oznámenie alebo vykonanie požadovaného opatrenia; alebo

b) odmietnuť konanie o žiadosti.

3.6. *Je povinnosťou žiadateľa podieľať sa na zverejňovaní?*

Áno, aj keď je povinnosť spolupracovať uvedená iba v odôvodnení 63, v doteraz publikovanej literatúre sa predpokladá predovšetkým to, že existuje (tak ako to bolo uznané aj v Rakúsku podľa DSG 2000): " čo sa týka dotknutej osoby, mohol by

[1] See also Souhrada-Kirchmayer, The right of access to the DSGVO, in Jahnel [Hrsg], Yearbook 17. Data Protection Law [2017] 86 f.

[2] See e.g. the jurisprudence of the Austrian High Courts: VwGH 4.7.2016, Ra 2016/04/0014; OGH 25.2.1993, 6 Ob 6/93)

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

prevádzkovateľ požadovať to, aby pred poskytnutím informácií dotknutá osoba špecifikovala informácie alebo spracovateľské činnosti, na ktoré sa žiadosť vzťahuje"[3]

3.7. Je potrebné brať do úvahy práva tretích strán?

Áno, podľa článku 15 ods. 4 GDPR právo na obdržanie kópie nesmie mať vplyv na práva a slobody ostatných. Navyše v odôvodnení 63 sa ďalej uvádza, že "právo by nemalo nepriaznivo ovplyvňovať práva alebo slobody iných, vrátane obchodného tajomstva alebo duševného vlastníctva, a najmä ochrany autorských práv softvéru, ale výsledok týchto úvah by nemal byť odmietnutie poskytnúť všetkým informáciám dotknutej osobe."

Preto je potrebné kontrolovať údaje, ktoré sa majú sprístupniť, spravidla musia byť osobné údaje tretích strán (napríklad meno osoby, ktorá sa zaoberá zákazníkom a uvedené v súbore zákazníka) vymazané z kópie údajov.

[3] Recital 63.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

4. Checklist for disclosing information on request

Musím poskytnúť informácie?	Ak je miestny verejný orgán správcom údajov - ÁNO. Ak je miestny verejný orgán iba spracovateľom, ale stále dostáva žiadosť, musí ho okamžite postúpiť zodpovednej osobe.
Overenie identity	Identita osoby, ktorá požaduje informácie (dotknutá osoba) musí byť jasná. Ak máte pochybnosti o totožnosti: Požiadajte o dôkaz
Je zverejnenie informácií bezplatné?	V zásade - ÁNO. Ak sa žiadateľovi často poskytli rovnaké informácie, alebo žiadosť vážne narúša práva kontrolóra, je možné, že sa spoplatní tento úkon. NB! Je to aj vecou štátnej jurisdikcie. Preto skontrolujte platné právne predpisy o vašej činnosti.
Sú osobné údaje žiadateľa spracované vôbec?	Ak neboli uchované žiadne údaje o žiadateľovi alebo ak údaje už boli vymazané alebo údaje boli nezvratne anonymizované, nebudú spracované žiadne osobné údaje a budú poskytnuté tzv. Negatívne informácie - "Neprocesáme údaje o vy ".
Aké údaje a informácie má kontrolór poskytnúť?	Všetky údaje musia byť poskytnuté, tie, ktoré sa týkajú príslušnej osoby. V závislosti od zložitosti systémov je potrebné vopred (v zmysle spracovateľského zoznamu) zvážiť, v ktorých systémových údajoch sa dá nájsť kategória postihnutých osôb. Okrem toho musia byť patričné informácie uvedené v článku 15 ods. 1 GDPR. Je potrebné dodržiavať práva tretích strán (najmä obchodné tajomstvá a údaje tretích strán musia byť vymazané / začiernené.

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

4.1. Východzie informácie

Príklad zverejnenia informácií podľa článku 15 GDPR

Vaša žiadosť o informácie

Vážený pán / pani [meno],

1. Vaša žiadosť od [dátum] na informácie podľa čl. 15 GDPR, ktoré sme dostali od [dátum], možno odpovedať nasledovne:

2. [V prípade odpovede v lehote jedného mesiaca od prijatia] Týmto potvrdzujeme, že spracovávame osobné údaje o vás.

[v prípade predĺženia podľa čl. 12 (3) GDPR] Ako bolo uvedené v liste z [dátum], využili sme možnosť predĺžiť lehotu na tri mesiace z dôvodu [zložitosti žiadosti alebo počtu vašich žiadostí, ďalšie vysvetlenie je potrebné].

3. [ak nie sú spracovávané žiadne údaje] Žiadne osobné údaje nebudú spracované. [Potom pokračujte textovým modulom č. 9].

[Pri spracovaní údajov] Konkrétne spracujeme nasledujúce údaje o vás: [Tu je zoznam aktuálnych údajov, ktoré sa majú spracovať].

Výtlačky / kópie z príslušného spracovania údajov nájdete v dodatku. Akékoľvek začiernenie ,alebo vynechanie bolo vykonané tak, aby neovplyvnilo práva a slobody iných, alebo z dôvodu, že sa informácie netýkajú vás alebo vašich osobných informácií.

4. [ak údaje neboli zhromaždené od dotknutej osoby]: Obdržali sme vaše dáta z [dostupných informácií o pôvode vašich údajov, napr. verejný orgán XY].

5. [ak to prichádza do úvahy] Budeme používať automatizované postupy rozhodovania / profilovania, ktoré majú na vás právne účinky, alebo vás podobným spôsobom ovplyvnia: [doplňte zmysluplné informácie o príslušnej logike a dôsledkoch a dôsledkoch].

6. Máte právo na opravu, vymazanie, obmedzenie a právo namietať na spracovanie svojich osobných údajov. Preto nás prosím kontaktujte. Ak sa domnievate, že spracovaním vašich údajov sa porušuje zákon o ochrane údajov, alebo ak boli inak porušené vaše nároky na ochranu údajov, môžete sa sťažovať na príslušný dozorný orgán. V tejto krajine za to zodpovedá XYZ.

S priateľským pozdravom

….

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

5. Externé zdroje a Webové Linky

5.1. Bibliografia a články

- Souhrada-Kirchmayer, The right of access to the DSGVO, in Jahnel [Hrsg], Yearbook 17. Data Protection Law [2017] 86 f.
- ***Martini in Paal/Pauly*** (Ed.), Datenschutz-Grundverordnung (2016).

5.2. Ostatné dokumenty a prípady

- jurisprudence of the Austrian High Courts: VwGH 4.7.2016, Ra 2016/04/0014; OGH 25.2.1993, 6 Ob 6/93) Web Links
- To compare the changes to directive 95/46/EC see https://gdpr.report/news/2017/11/20/gdpr-subject-access-requests/

The content of this publication represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).