Introduction to Personal Data Processing

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

GDPR key points

- **Direct application:** the provisions of the GDPR are directly applicable to all European citizens and institutions even without national legislation in the field of data protection
- **Applicable from:** 25th May 2018
- **Significance:** the GDPR introduces a lot of new notions, such as new obligations for data controllers and data processors; however, some notions such as the legal grounds for processing remain unchanged in comparison to the previous regime

GLOSSARY

Personal data:

- Personal data is any information relating to an identified or identifiable natural person (data subject);
- A natural person is identifiable when there is a possibility to be identified and distinguished from all other members of a group;
- The data should be related to a living person; data of deceased persons is outside the scope of the GDPR;
- Identifiers (means for identifying the subject) may be name, identification number, location data, an online identifier or factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity.

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

GLOSSARY

Processing of personal data:

- any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

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

GLOSSARY

Data controller:

- the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; the purposes and means may be determined by EU or national law, when the controller or the specific criteria for its nomination are provided for by EU or national law.

Data processor:

- a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

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

GLOSSARY

Data subject:

- A natural person about whom data is processed;
- NB! All natural persons who are EU citizens fall under the term.
- NB! All natural persons who are living in the EU fall under the term.

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

Legal Grounds for Personal Data Processing

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

LAW AND INTERNET FOUNDATION

LATVIAN ASSOCIATION OF LOCAL AND REGIONAL GOVERNMENTS

SMA THE EXTENDED ENTERPRISE

SNSPA

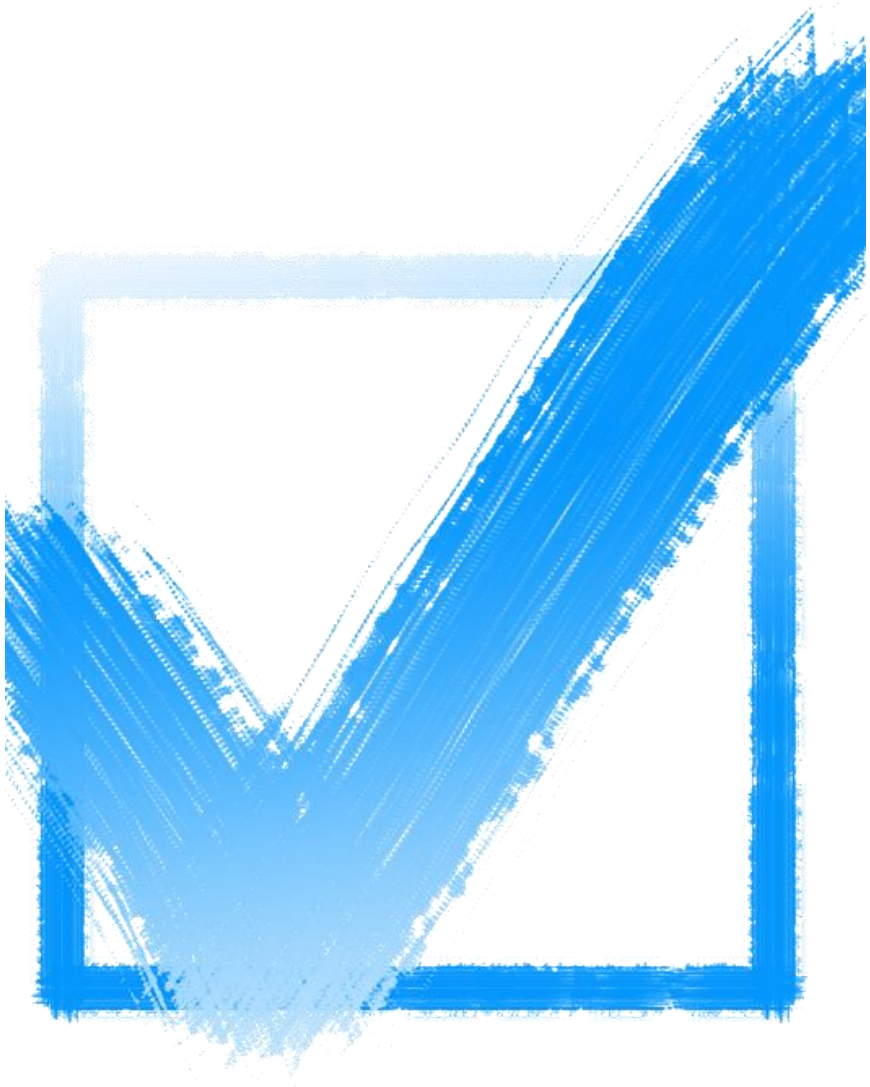
The processing is considered lawful on 6 grounds (Art. 6 GDPR) :

1. Consent of the data subject;
2. Performance of a contract to which the data subject is party / taking steps at the request of the data subject before entering into a contract;
3. Legal obligation of the controller;
4. Protection of the vital interests of the data subject or of another natural person;
5. Performance of a task of public interest / exercise of official authority vested in the controller;
6. Legitimate interests of the controller or a third party.

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

Consent

- **Freely-given** – the data subject must have real choice and control;
- **Specific** – the subject has to consent his/her data to be processed for a specific purpose;
- **Informed** – GDPR requires what type of information should be provided to the subject;
- **Unambiguous** – consent must be given with a clear, affirmative act;
- **Consent could be withdrawn at any time**;
- **Consent of children** – in cases of providing information society services, the consent is given by the holder of parental rights.



Consent in the context of local authorities' activities

- Narrowly used as in most cases citizens are in a subordinate position to public authorities and consent is not a suitable basis for personal data processing;

- Consent might be used in situations in which local authorities either do not exercise their typical and main functions or the processing is optional (such as sending information to citizens about administrative procedures or activities organised by the local authorities).

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

Conclusion & Performance of a contract with the data subject

This basis is used in two cases:

- situations where the processing that takes place *prior to* entering into a contract; this covers pre-contractual relations, when steps are taken at the request of the data subject.
- situations where the processing is necessary for the performance of the contract to which the data subject is a party;

Conclusion & Performance of a contract with the data subject in the context of local authorities

In exercising their powers, local authorities can use this basis for processing in situations as:

- processing in the employment context – processing of salary information and bank account details;
- processing in the context of conclusion of public procurement contracts (NB! with a data subject, not with a legal entity);
- processing in the context of relationships between private entities owned by the municipality, and the citizens.

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

Legal Obligation

A controller can process data on this basis when there is a legal provision which is:

- part of EU or national legislation;
- on legislative or on sub-legislative level;
- clear and precise;
- compliant with data protection acts, including the requirement of necessity, proportionality and purpose limitation;
- imposing obligation to the controller.

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

Legal obligations in the context of local authorities' activities

- One of the most important legal grounds for personal data processing conducted by local authorities;
- Covers both processing related to providing administrative services/ facilitating the performance of public obligations of the citizens and fulfilling obligations of the local authorities in their capacity of employers.

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

Vital interest

- Used only where the processing cannot be **manifestly** based on another legal basis;
- Vital interest either of the data subject or of another natural person;
- Has limited application – e.g. when there is imminent threat for fundamental rights of the subject;
- Includes processing 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.

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

Vital interest in the context of local authorities' activities

Could be applied in a very limited number of cases

Example: processing personal data of employees or citizens in case of emergency situations occurred under the jurisdiction of a local authority and there is no other legal ground for such processing.

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

Task carried out in the public interest & exercise of official authority

- The processing should be laid down in EU or national law;
- Situations in which a party that is not a public authority is requested to disclose personal data to a public authority are no longer in the scope of this basis;
- Data subjects could object to processing on this basis;
- In case of objection: Local authorities should be able to demonstrate that they have compelling legitimate grounds to process the personal data further on this basis.

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

Tasks of public interest & exercise of official authority in the context of local authorities' activities

- One of the most important legal grounds for the LAs' activities;

- **Examples**:
  - when administering local taxes;
  - when administering a local library, school, etc.

Legitimate interest

- The concept of interest – “broader stake that the controller derives from the processing”;
- Legitimacy of the interest – when it is compliant with both data protection laws and the laws applicable to the activity of the controller;
- The legitimate interest should override the interests, fundamental rights and freedoms of the data subject

=

<u>a balancing test should be applied on a case by case basis</u>

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

Legitimate interest in the context of local authorities' activities

- GDPR explicitly provides that this legal basis shall not apply to processing carried out by public authorities in the performance of their tasks;
- It is advisable for local authorities that rely on legitimate interest for performing their tasks to reconsider which other legal ground for personal data processing they could apply;
- The legitimate interest could still be applied by local authorities as a valid legal ground for their internal processes – for example in their HR activities.

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

GDPR myths

- X Data subjects must give consent for every processing operation – consent should be used only when there is no other legal basis for processing; its use should be limited, especially by public authorities;
- X Legitimate interests could not be legal basis for processing by public authorities – it is important always to consider the role in which the local authorities are acting;
- X Compliance with a legal obligation is always the basis for processing by public authorities – in a lot of cases local authorities will not be obliged to process certain set of data, but instead will exercise its official authority.

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

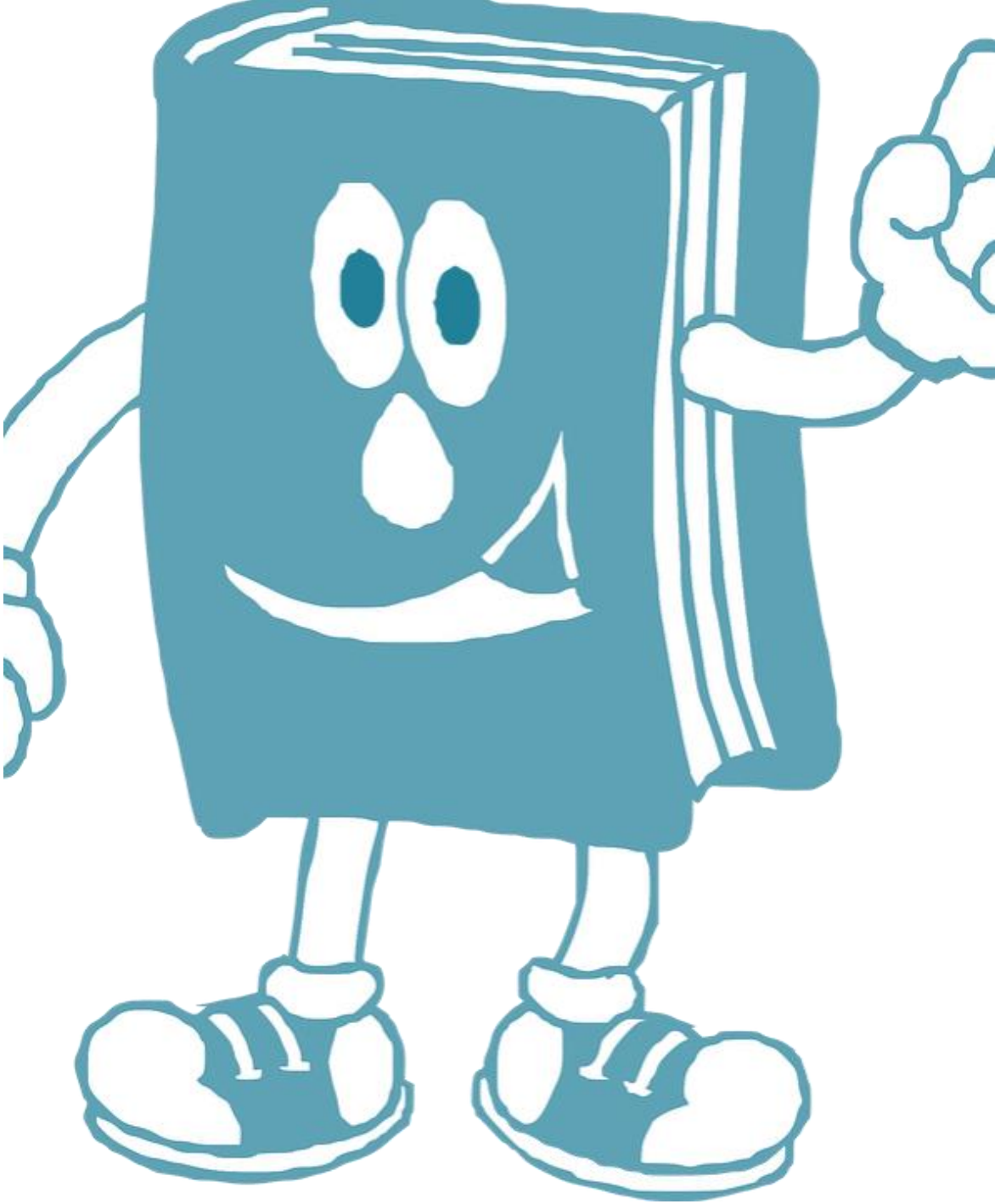
Conclusion

- The data controller should always determine the legal grounds for each processing activity it performs;
- The information which legal ground applies to which purpose of processing should always be provided to the data subject;
- Local authorities should mostly rely on the legal grounds “performing tasks in the public interest/exercise of official authority” and “complying with legal obligation; however, in certain situations other legal grounds may be applicable.

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

Suggestions for further readings:

- When can personal data be processed?
- 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;



Processing of Special Categories of Personal Data

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

Glossary

- **Special categories of data**:
  - personal data which, by their nature, are particularly sensitive in relation to fundamental rights and freedoms
  - such data merit specific protection as the context of their processing could create significant risks to the fundamental rights and freedoms

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

The logic behind defining certain categories of personal data as special

- **Directive 95/46:** the first EU legal act devoted to personal data protection outlined:
  - "Risky" categories of personal data: certain categories of personal data that could entail higher risk for the fundamental rights and freedoms of the European citizens;
  - They are also 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;
  - Processing of such data is prohibited and such data could be processed only in exceptional circumstances, exhaustively listed in the data protection legislation of the Member States.

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

Special Categories of Personal Data under GDPR

- GDPR 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;
- Different types of data have different impact of the individuals (i.e. objective approach);
- The choice which categories of personal data to be defined as special was substantially influenced by anti-discrimination law.

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

TYPES OF SPECIAL CATEGORIES OF PERSONAL DATA

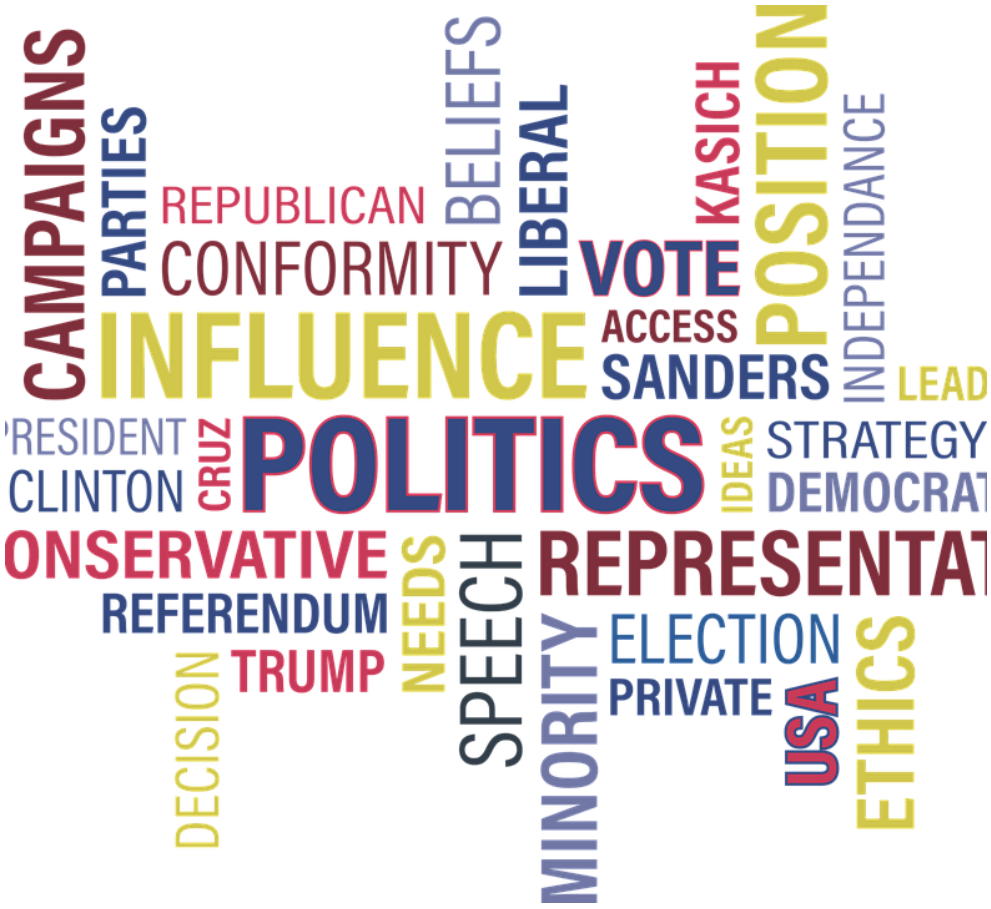
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

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, his place of birth, his native language or the names of his parents that might, when combined, allow conclusions as to his origin.

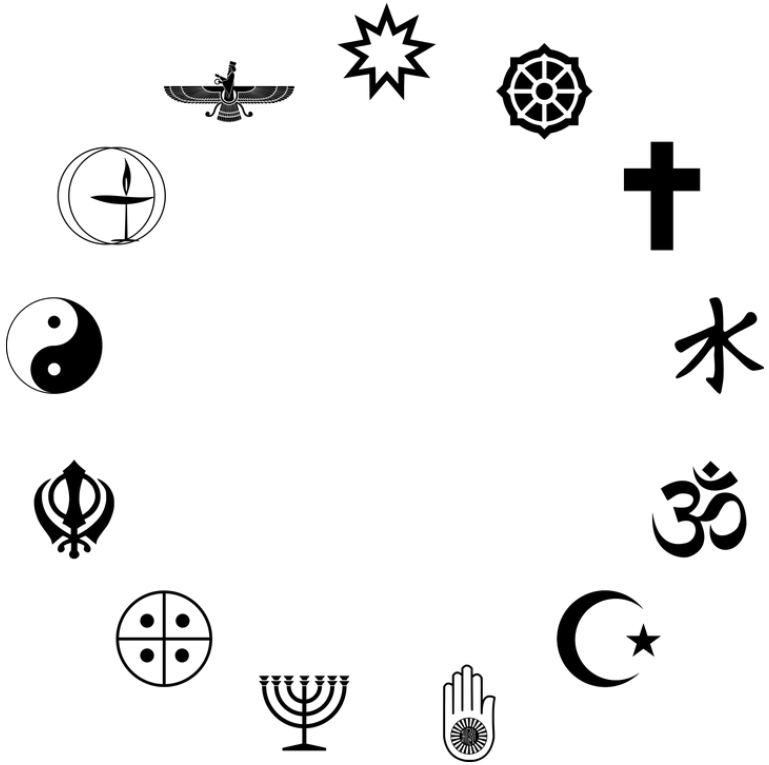
Political opinion

- 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.



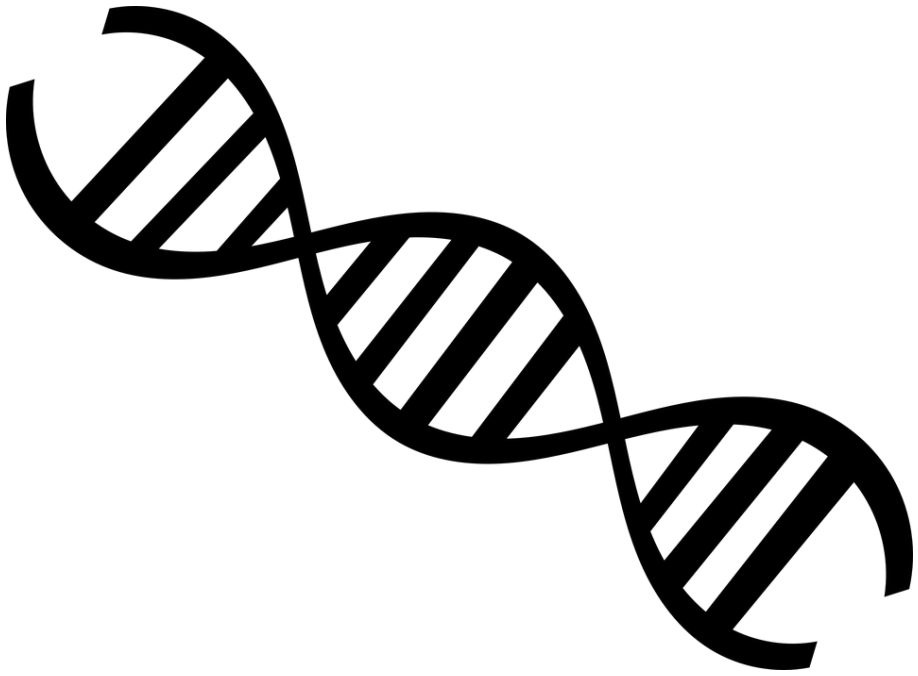
Religious or philosophical beliefs

- 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 and action, and thus, should not be unequally treated on the basis of their trade union affiliation.



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 gives 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, but GDPR for first time introduces it on EU level.
- Genetic data should be protected, as 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 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 behavioural 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), 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.

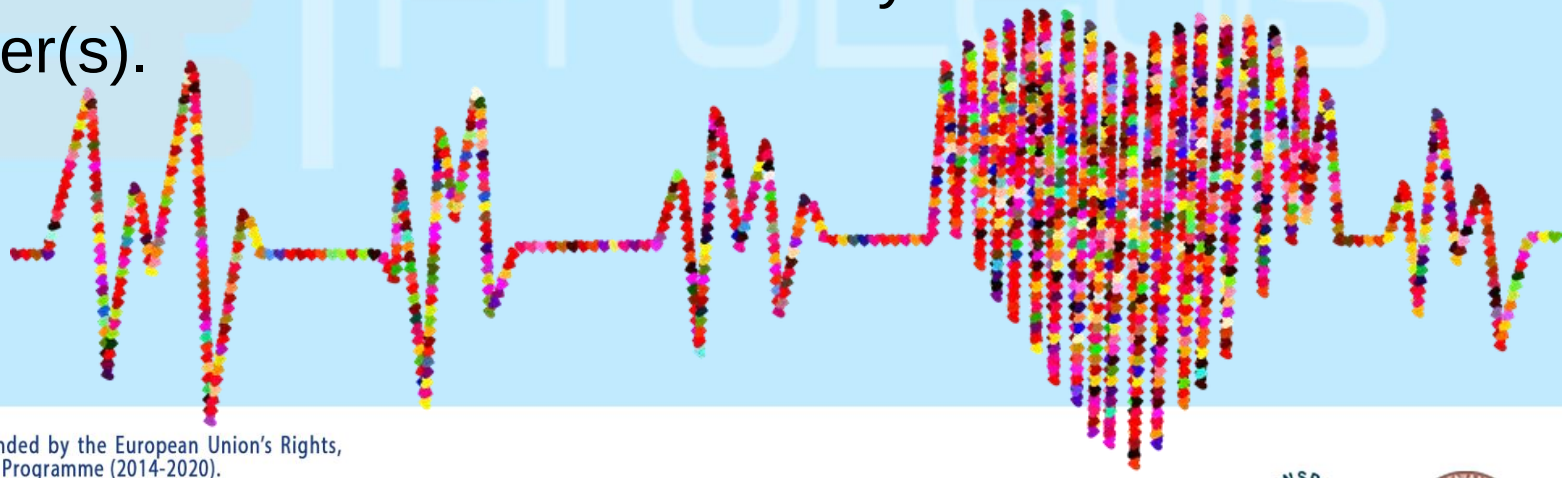
Biometric data for the purpose of uniquely identifying a natural person

- 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).

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

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).



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

LAW AND INTERNET FOUNDATION

LATVIAN ASSOCIATION OF LOCAL AND REGIONAL GOVERNMENTS

SMA THE EXTENDED ENTERPRISE

SNSPA

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.

- 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.

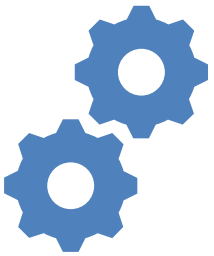
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

Personal data relating to criminal convictions and offences

- 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:
  - The processing should be under the control of official authority; or
  - The processing is authorised by EU/ Member State law providing for appropriate safeguards for the rights and freedoms of data subjects.

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

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 in Art. 9 is fulfilled.
- The conditions are indicated in the next slides.

Explicit consent

- The requirements that must be met under GDPR in order to have a valid consent (freely given, specific, informed, unambiguous) apply in any case for processing of special categories personal data.
- The term ‘explicit’ refers to the way consent is expressed by the data subject – the data subject must give an express statement of consent.
  - One of the ways to give consent is to expressly confirm it in written statement;
  - In an 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.

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

Explicit Consent

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

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

Obligations & specific rights in the field of employment, social security and social protection law

- Especially relevant for local authorities when managing their internal HR process. Processing of special categories of personal data might be necessary at every stage of the labour 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 labour relationship, etc.

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

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

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

- The processing must be necessary to perform an obligation of the data controller or a certain right of the data subject;
- This obligation / right could be provided in EU/ Member State law or in a collective (bargaining) agreement;
- There should be appropriate safeguards for the fundamental rights and the interests of the data subject.

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

Vital interests of the data subject or of another natural person

- Similar to the legal ground under *Art. 6 of GDPR*, “vital interest” refers to circumstances of life or death;
- 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 implies that <u>the controller should try to obtain the consent of the data subject first.</u>

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

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 organisations such as political parties, foundations, churches, other forms of philosophical, religious or trade union organisations. Such organisations could process sensitive data if:

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

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

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 such information;
- The decision to disclose such information needs to be result of the individual's free choice;
- 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.;
- 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 data protection by default & data protection by design, taking appropriate measures to guarantee the security of the data, etc.

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

Establishment, exercise or defence 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;
- Such situations might include e.g. appeals before administrative courts of acts issued by the local authorities where processing of sensitive data took place in the preceding administrative procedure; labour disputes where the health data of the employees should have been taken into account by the local authority as an employer, etc.;
- Furthermore, the processing within the judicial activities of courts could also substantiate processing of such categories of personal data.

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

- Member States are authorised to introduce into their national legislation specific hypothesis where sensitive data could be processed due to justified substantial public interest;
- To meet the requirements of GDPR, the Member States must ensure that:
  - the processing should be proportionate to the aim pursued;
  - the essence of the right to data protection is respected;
  - the legislation adopted provides for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

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

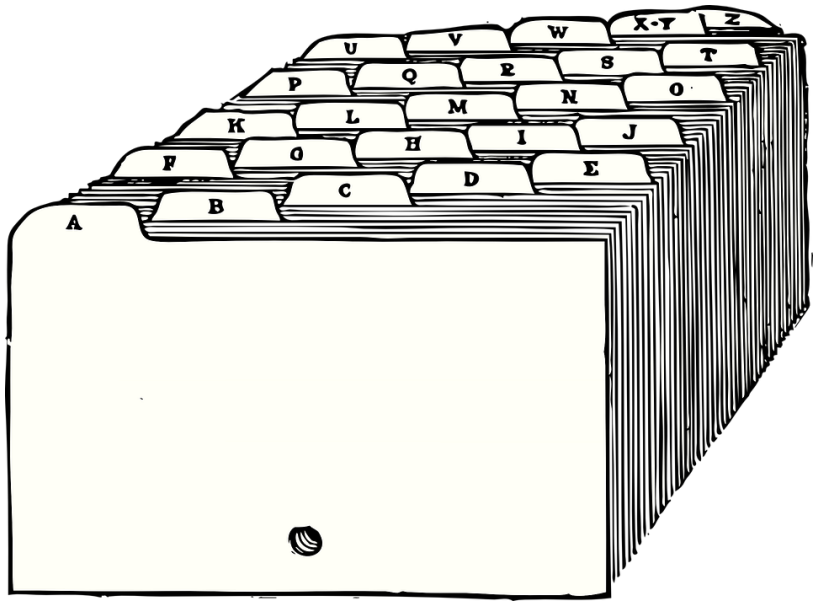
Preventive or occupational medicine, assessment of the working capacity of the employee, medical diagnosis, provision of health or social care or treatment

- The prohibition to process special categories of personal data does not apply to processing for medical/ social care purposes;
- 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;
- 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.

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.
- 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.

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



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 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.

Further conditions in national law

Art. 9, Para 4 of GDPR authorises 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.

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

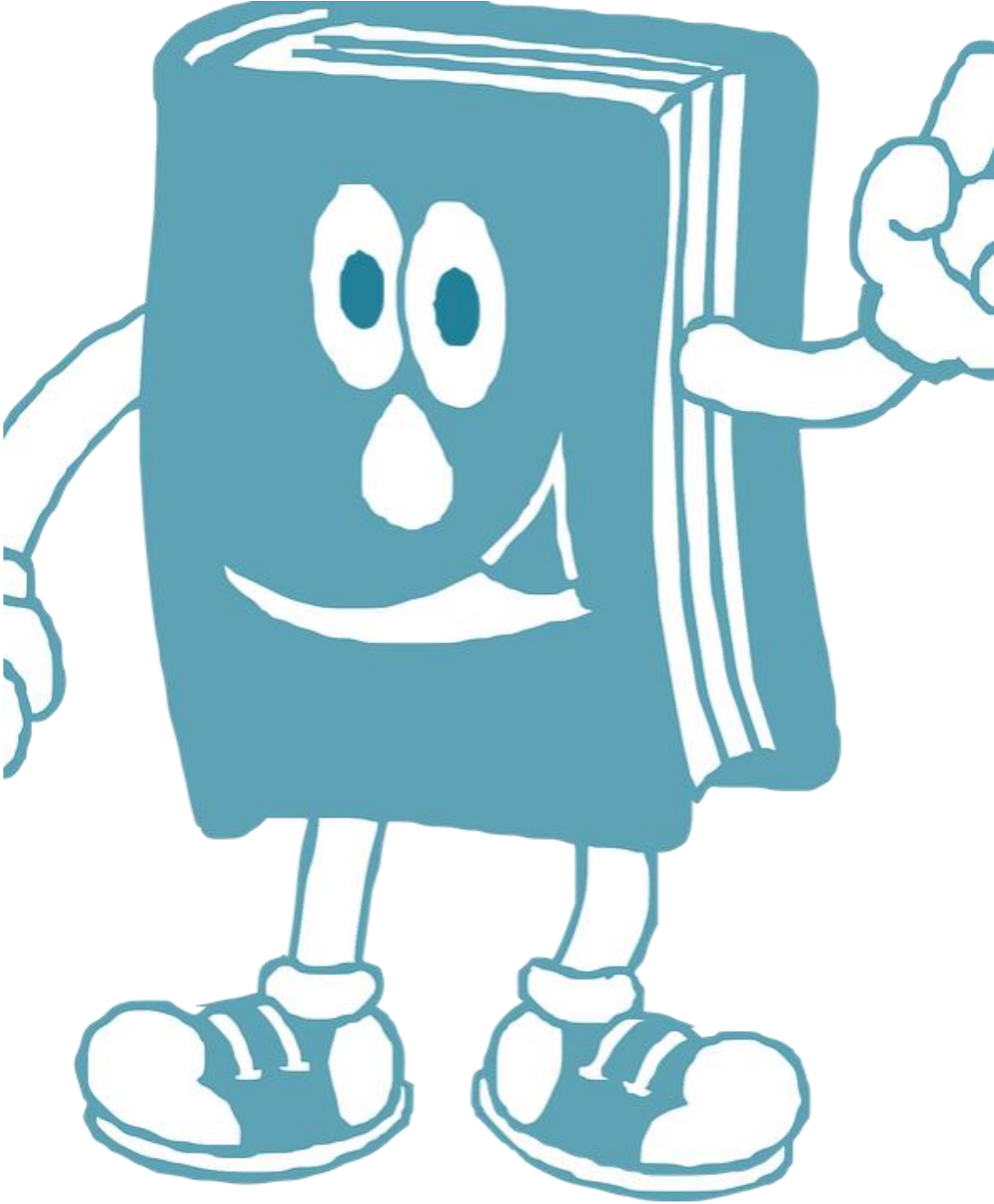
Conclusion

- Local authorities 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 local authorities' 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.

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

Suggestions for further reading:

- What personal data is considered sensitive?
- Under what conditions can my organisation process sensitive data?
- 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;



Data Protection Management

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

Principles relating to processing of personal data

Article 5 GDPR

(1) personal data shall

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

(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes (‘purpose limitation’);

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (‘data minimisation’);

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (‘accuracy’);

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

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

Principles relating to processing of personal data

e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation');

f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

(2) The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability').

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

Responsibility of the controller

Article 24 GDPR

(1) Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary.

(2) Where proportionate in relation to processing activities, the measures referred to in paragraph 1 shall include the implementation of appropriate data protection policies by the controller.

(3) Adherence to approved codes of conduct as referred to in Article 40 or approved certification mechanisms as referred to in Article 42 may be used as an element by which to demonstrate compliance with the obligations of the controller.

Data Protection Management System (DPMS)

- Goal: that employees' compliance with the strict requirements of the GDPR in the processing of personal data is not left to chance.
- The data protection principles should always be respected
- It is for this purpose, that the various instruments of controlling an organisation are to be designed.

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

LAW AND INTERNET FOUNDATION

LATVIAN ASSOCIATION OF LOCAL AND REGIONAL GOVERNMENTS

SMA THE EXTENDED ENTERPRISE

Different roles in GDPR

The GDPR recognises the following data protection roles:

- **Controller** (Art 4 No 7)
- **Joint controllers** (Art 4 No 7 in conjunction with Art 26)
- **Processor** (Art 4 No 8)
- **Data Subject** (Art 4 No 1)
- **Recipient** (Art 4 No 9)
- **Third party** (Art 4 No 10)

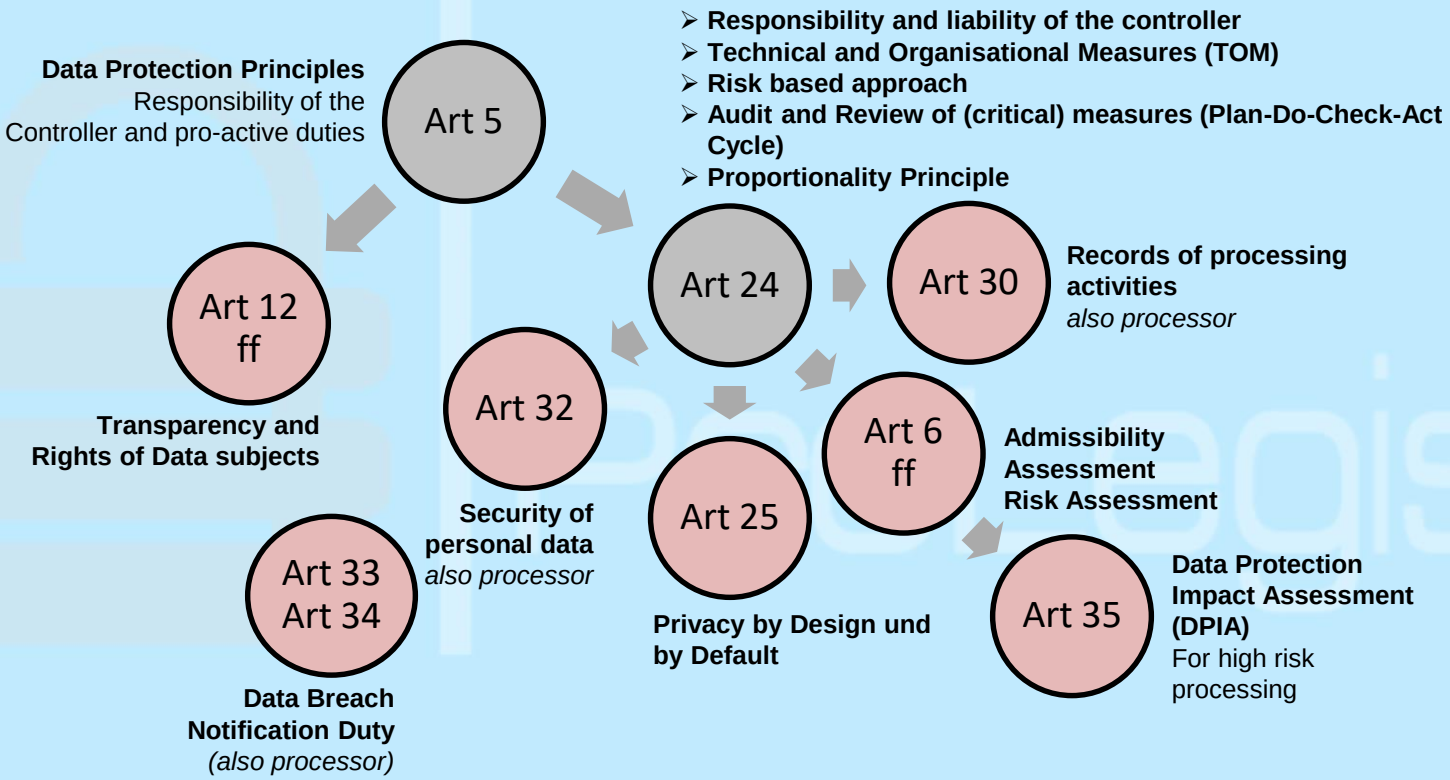
This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

Data Protection Principles according to GDPR

- **Principle of lawfulness**
- **Principle of transparency**
- **Purpose of limitation**
- **Data minimization principle**
- **Principle of accuracy**
- **Principle of storage limitation**
- **Data Protection by Design and Data Protection by Default**
- **Principle of empowering data subjects**
- **Principle of data security**
- **Principle of accountability**
- **Prohibition principle**

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

Overview of the controller's obligations

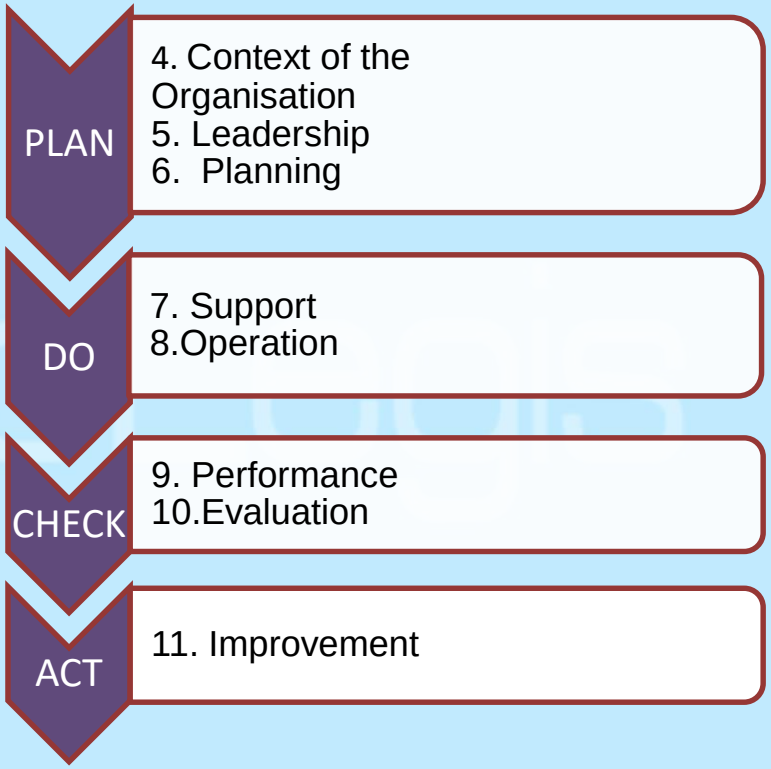


This publication was funded by the European Union's Rights, Equality and Citizenship Programme (2014-2020).

High Level Structure

- ISO Standards for different kinds management systems are **basically built on a generic structure:**
  - ISO 9001:2015: Quality Management System
  - ISO 27001:2013: Information Security Management System
  - ISO 27552 (draft version)
- Standards have high synergies
- One Management-System for all different topics to handle
- Generic structure for generic requirements: „How do we manage to get properly done what we are supposed to do as an organisation?“

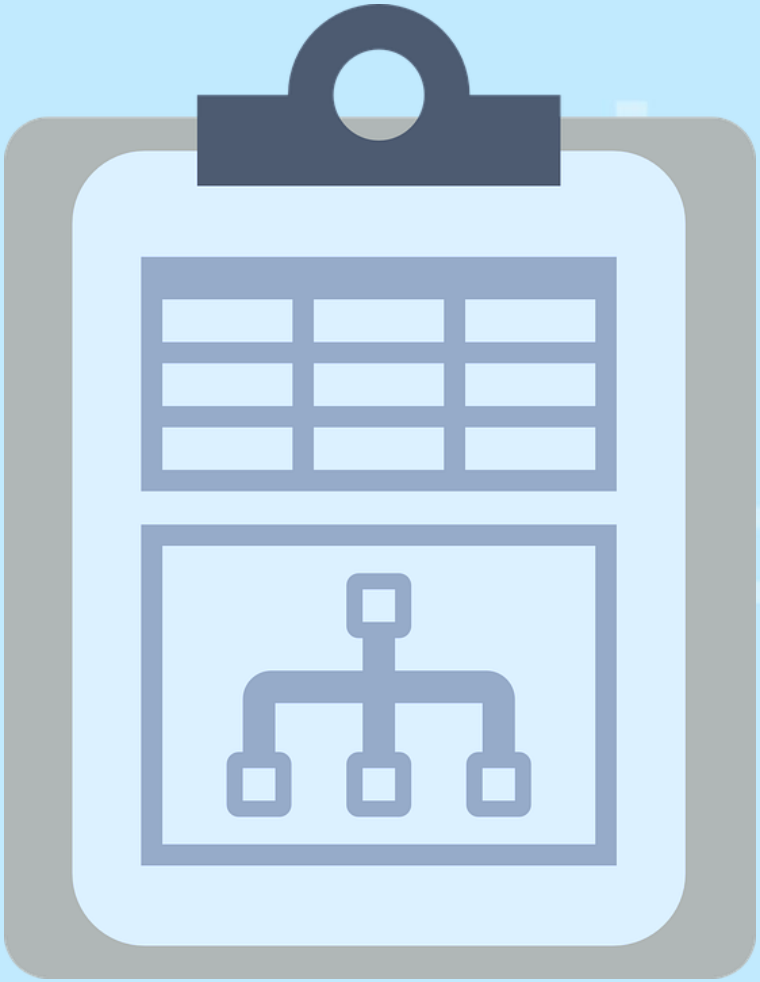
1. Scope
2. Normative references
3. Terms and definitions



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

LATVIAN ASSOCIATION OF LOCAL AND REGIONAL GOVERNMENTS

Conclusion and Practical Tips



The following practical steps should be undertaken:

- Customisation or creation of a privacy policy;
- Adaptation or creation of concrete measures and corresponding instructions;
- Establish internal control system or extend existing system to data protection;
- Work with tailored forms, checklists, SOPs, etc. as much as possible;

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

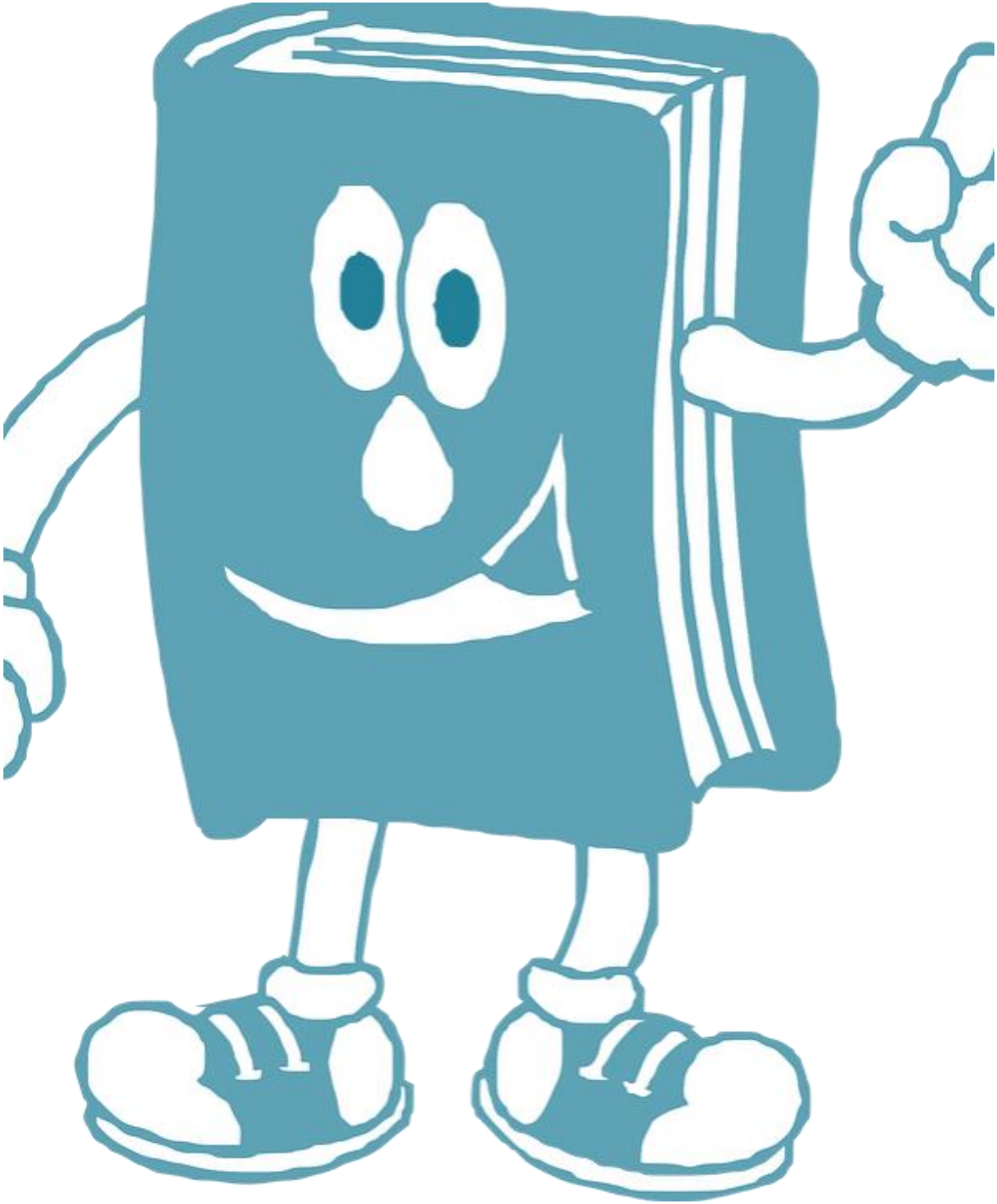
Conclusion and Practical Tips

The following practical steps should be undertaken:

- Establishment of record of processing activities as a basis for data protection management > therefore not only compulsory content but also other elements, e.g. the software / hardware used for data processing.
- Keep the overhead as low as possible: just refer to existing documentation (e.g. IT security guideline) and do not rewrite everything
- Set up a data protection coordination group in the organization that includes several people in different roles (e.g. IT manager, legal department, HR department, quality manager, marketing, etc.).

Suggestions for further reading:

- Paul Voigt, Axel von dem Bussche, The EU General Data Protection Regulation (GDPR): A Practical Guide (English), 2017;
- Brussels Laboratory for Data Protection and Privacy Impact Assessments;
- German “TÜV Nord”.



Designation, Position and Tasks of Data Protection Officers

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

Glossary

- Data protection officer (DPO) – a position within an organisation with the primary task to monitor if personal data is handled in compliance with the data protection legislation.

Mandatory appointment

- When the controller is a public authority or body;
- When the core activities of the controller/ processor […] require regular and systematic monitoring of data subjects on a large scale;
- When the core activities of the controller/ processor consist of processing on a large scale of special categories of data […] OR personal data relating to criminal convictions and offences;
- When provided for in EU and/or national law.

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

Mandatory appointment by public authorities

- The scope of this requirement may also include certain natural/ legal persons whose activities are governed by public law and are connected to the provision of public services to citizens (public transportation);

- It is recommended as a good practice to designate a DPO whose functions cover all processing operations carried out, including those that are not related to the performance of a public task or exercise of official duty.

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

Voluntary appointment

The voluntary appointment might be applied to certain organisations whose capital is owned entirely or partially by the municipality – i.e. infrastructure construction company.

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

How to designate a DPO?

OPTIONS FOR CONTRACTUAL RELATIONS WITH THE DPO

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

Labour contract

There are two possibilities:

1. To appoint somebody already working in the organisation to combine their function with the functions of the DPO → better choice for smaller organisations;

2. To open a new working position for the DPO → better choice for bigger organisations;

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

Service contract

- The Regulation explicitly provides that the function of DPO may be outsourced to external individual/ organisation under a service contract;
- It is recommended 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;
- Each member of the external DPO organisation should fulfil all applicable requirements under the GDPR;
- Concluding a service contract with an external DPO might require the conducting of certain formal procedures (e.g. under public procurement law).

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

The position of the DPO

Involvement in all issues related to personal data protection

- The DPO should be involved in each process that includes personal data processing from the earliest stage possible as one of the tools to ensure data protection by design.

Involvement in all issues related to personal data protection

- The involvement of the DPO could constitute in:
  - advice during the conduct of data protection impact assessment;
  - participation in work meetings;
  - consultation on management decisions regarding data processing and measures in case of a data breach;
  - maintenance of the records of processing activities.

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

Necessary resources

- The management of the organisation is responsible to ensure that the DPO is properly secured at least in terms of:
  - organisational matters – a team, access to other teams, accountability only before the highest management and others;
  - financial matters – financial resources and facilities;
  - education matters – courses, new literature and others.

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

Independence

- The DPO should not receive any instructions regarding the exercise of their tasks regarding the implementation of data protection;
- The DPOs must not be sanctioned or suffer any unfavourable consequences as a result of the performance of their tasks.

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

Conflict of interests

- If the DPO is designated under a labour contract, this designation should not result in conflict of interests:
  - the DPO should not determine the means and purposes of processing while executing their other functions;
  - the DPO should not hold a managing position of any kind.

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

Conflict of interests

- Conflict of interests may arise also for an external DPO;
  - **Example:** when the DPO is asked to represent a controller and a processor before a court and they have contradicting interests.

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

Tasks of the DPO

Monitoring

- One of the key tasks of the DPO is to monitor all data processing activities within the organisation, which includes:
  - receiving/ collecting of information;
  - internal analysis of this information and making clarifications;
  - check of the compliance of ongoing processing activities;
  - recommendations and giving advice within the organisation.

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

Data Protection Impact Assessment (DPIA)

- DPOs should be involved in the DPIA with advisory functions on issues as:
  - whether to carry out a DPIA at all;
  - what methodology to follow when carrying out a DPIA;
  - what safeguards to apply;
  - whether the DPIA has been correctly carried out.

- Good practice: documenting and justifying decisions when they deviate from the advices of the DPO.

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

Contact point

- The DPO is a contact point for both:
  - the supervisory authority; and
  - data subjects.
- The requirement to provide the DPO's contact details is one of the elements of the transparency principle;
- The GDPR does not preclude the DPO from seeking advice from the supervisory authorities.

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

Record keeping

- GDPR does not encompass provisions that preclude organisations to assign the function of record keeping records to the DPO;
- The allocation of the recording keeping obligation to the DPO is considered as one of the tools enabling the DPO to perform its tasks;
- It is advisable to delegate this task to the DPO.

Myths about the DPOs under GDPR

- X Only natural persons could be DPOs – the functions of the DPO could also be fulfilled by organisations;
- X The legal advisers or the head of human resources of the local authorities can be appointed as DPOs – this would cause a conflict of interests;
- X The DPO bears the responsibility for compliance with the data protection legislation – the responsibility for compliance is still of the data controller or processor.

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

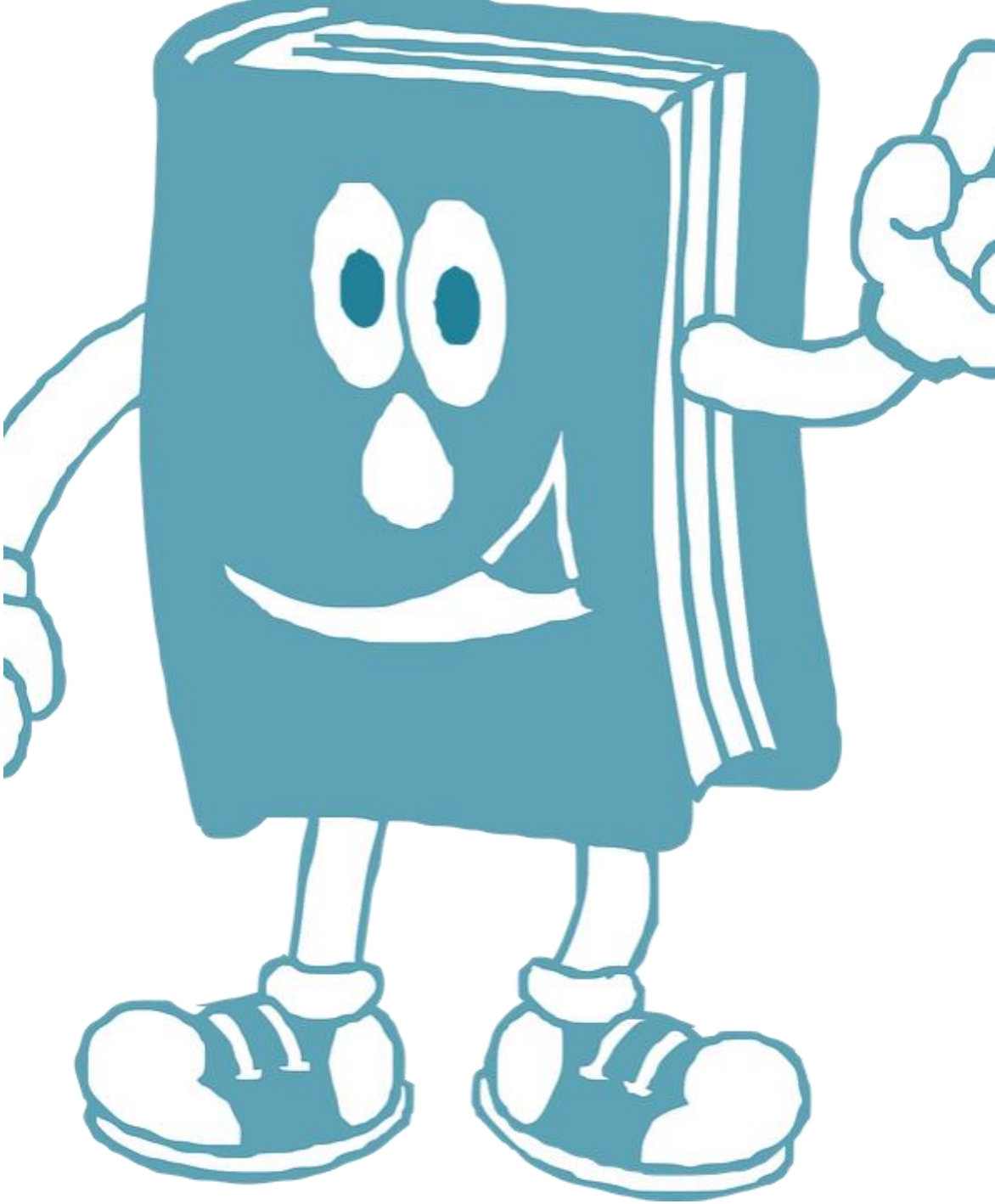
Conclusion

- The DPO is a key figure in ensuring GDPR compliance;
- As public bodies local authorities are obliged to appoint a DPO;
- Local authorities can choose between appointing a DPO, delegating the DPO's functions to a current employee or concluding a service contract with external DPO;
- Local authorities should be careful to avoid conflicts of interests when appointing a DPO.

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

Suggestions for further reading:

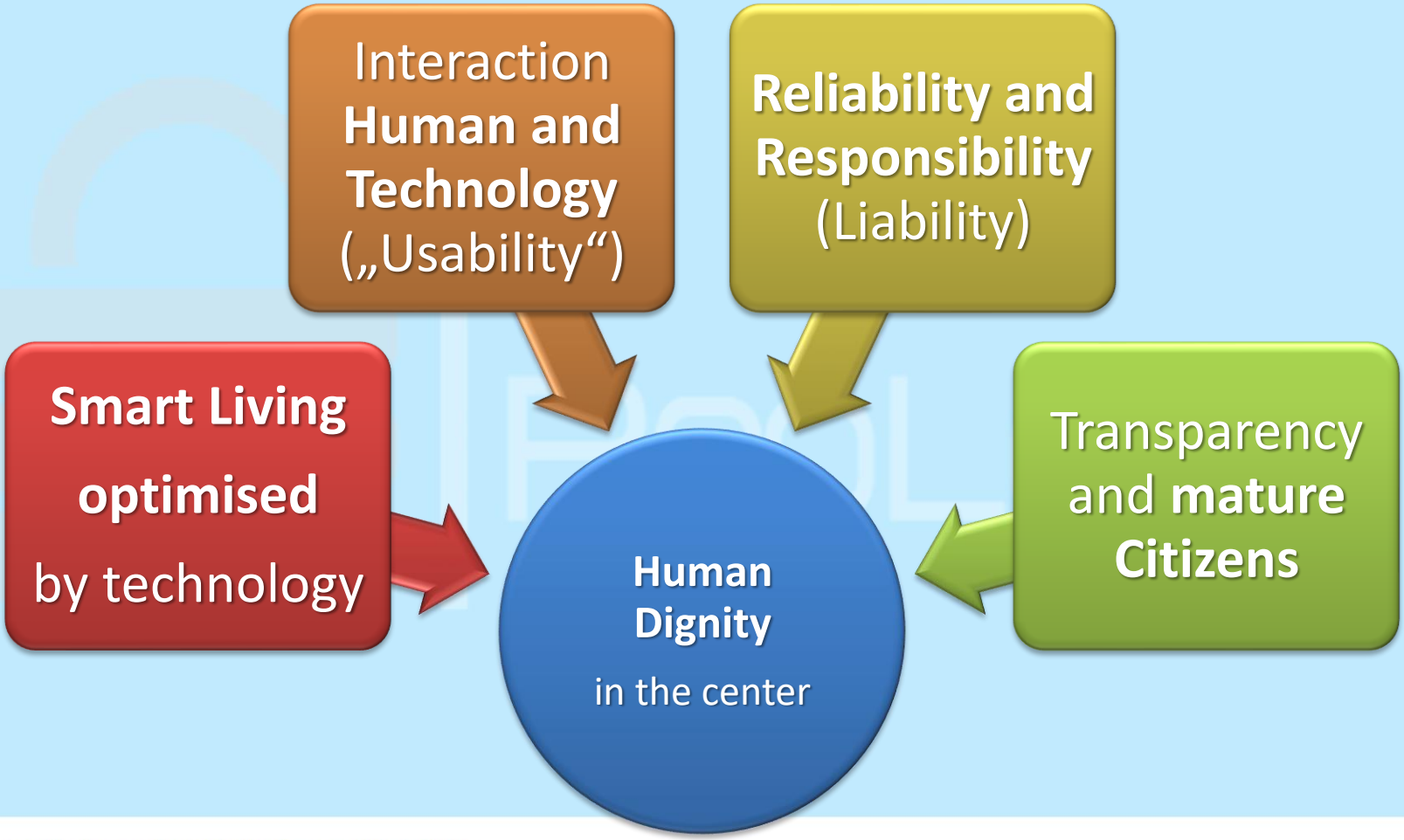
- WP29, Guidelines on Data Protection Officers (‘DPOs’), WP 243 rev.01



Data Protection Impact Assessment

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

The need for an impact assessment from the perspective of data subjects



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

LAW AND INTERNET FOUNDATION

LATVIAN ASSOCIATION OF LOCAL AND REGIONAL GOVERNMENTS

SMA THE EXTENDED ENTERPRISE

SNSPA

Data Protection Impact Assessment (DPIA): Intention of Art 35 GDPR

- GDPR replaces the obligation to register and to get an approval by the Data Protection Authority (Recital 89: "bureaucratic")
  - Responsibility of the controller and risk-based approach;
  - Intensive consideration of those processing activities that are likely to result in a high risk to the rights and freedoms of natural persons.

Data Protection Impact Assessment (DPIA): Intention of Art 35 GDPR

- Check if there is a high risk → based on that "threshold analyses":
  - Conduct DPIA;
  - Required documentation (recommended – in writing).
- The controller has to make the necessary concessions and assessments.
- If, based on the knowledge available at the time of the assessment, their inaccuracy was not foreseeable → No violation of duty.

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

LAW AND INTERNET FOUNDATION

LATVIAN ASSOCIATION OF LOCAL AND REGIONAL GOVERNMENTS

SMA THE EXTENDED ENTERPRISE

SNSPA

Art 35 in relation to other parts of GDPR

Risk analysis also required

- Art 25
  - Data protection by design and by default
    - Data Protection by Design as **an important measure to reduce risks**
- Art 32
  - Security of processing
  - Risks from Abuse and External Attacks
- Art 35
  - Also risks from the planned processing itself, not just from security breaches

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

Data protection by design and by default (Art 25 GDPR)

- Data protection by design and by default as new principles laid down in Art. 25 GDPR
- Systematic Approach for compliance with data protection law and for mitigation / elimination of risks
- Duty to "implement appropriate technical and organisational measures", in order to
  - implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing
  - meet the requirements of this Regulation and protect the rights of data subjects

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

Data protection by design and by default (Art 25 GDPR)

- Combined with mandatory data protection impact assessment (Art 35 GDPR) and strong rules on compensation and liability (Art 82)
  - Companies / Organisations recognise thus a "business case" for data protection
  - Necessary interdisciplinary skills are rarely and high valuable
  - therefore first time there is a high level market for human rights protection

Cases when a DPIA is mandatory (Art 35 Sec 3)

- 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.

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

LAW AND INTERNET FOUNDATION

LATVIAN ASSOCIATION OF LOCAL AND REGIONAL GOVERNMENTS

SMA THE EXTENDED ENTERPRISE

Cases when a DPIA is mandatory (Art 35 Sec 3)

- processing on a large scale of special categories of data referred to in Article 9 para 1, or of personal data relating to criminal convictions and offences referred to in Article 10:
  - When is processing to be considered “on a large scale"?:
  - Amount of data
  - Number of persons affected: reference value> 5000 within 12 months (thus, not e.g. a single doctor or a single lawyer)
- a systematic monitoring of a publicly accessible area on a large scale.

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

Further cases requiring a DPIA (Recital 91)

- Processing operations:
  - 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;
  - which involve a high level of risk and make it difficult for data subjects to exercise their rights;
  - 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 categories of personal data, biometric data, or data on criminal convictions and offences or related security measures;
  - 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;
  - which pose a high risk because they are systematically large scale.

Criteria for a „high risk“ according to Art. 29 Working party

Basic rule: A high risk exists if at least two of the following nine criteria are met:

- Evaluate or grading (profiling / scoring of natural persons)
- Automated decision-making with legal effect or similar significant impact
- Systematic monitoring
- Confidential data or sensitive personal data (Art. 9, 10)
- Large scale data processing (Recital 91)
- Match or merge records
- Data on vulnerable persons (Recital 75)
- Innovative use or application of new technological or organizational solutions
- Data processing that prevents parties from exercising a right or use of a service or performance of a contract (Art. 22, Recital 91)

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

Positive and negative lists for a DPIA

- The supervisory authority **must** compile a list of processing operations for which a privacy impact assessment is to be carried out (positive list).
- The supervisory authority **may** draw up a list of the types of processing operations for which no privacy impact assessment is to be carried out (negative list).
- Coherence procedure (Art. 63) for the coordination of these lists between the supervisory authorities regarding types of processing operations affecting several Member States for the purpose of uniform application of the GDPR

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

Timing for a DPIA

- Timing and method applied for a DPIA have to be determined by the controller
- It is recommended to start preparation for DPIA at the earliest possible stage of a project. Training is recommended to raise awareness about the need for DPIA within the organisation
- DPIA can guide the search for adequate solutions and can help to implement data protection requirements effectively
- 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.

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

Review of DPIA

- 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 materialize, a new DPIA has to be performed.
- 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.

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

Consultation with data protection authority pursuant Art 36 GDPR

- The data controller has to consult with the Data Protection Authority (DPA) when the DPIA reveal **major 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.

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

LAW AND INTERNET FOUNDATION

LATVIAN ASSOCIATION OF LOCAL AND REGIONAL GOVERNMENTS

SMA THE EXTENDED ENTERPRISE

SNSPA

Who is responsible to conduct a DPIA

- The responsibility of conducting a DPIA is with the controller.
  - 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 practice: appropriate to contractually require a processor, if available and already selected, to the involvement and active support throughout the DPIA process.
  - This beyond Article 28 (3) (f), which provides that the contract on the processing should provide for the processor to ensure compliance with the obligations Articles 32 to 36.

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

Minimum requirements for DPIA

Article 35, para 7, lit. a to d GDPR in conjunction with Recitals 84 and 90 requires as minimum:

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

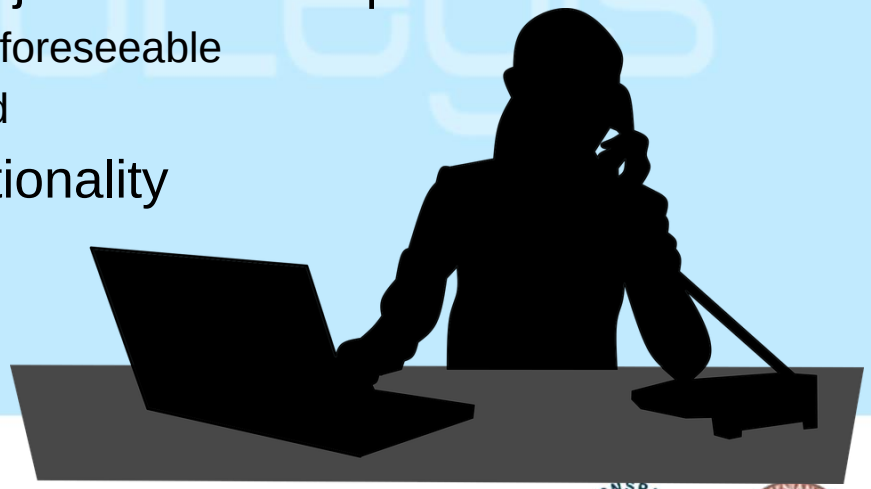
d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.

Letters c and d are manifestations of the GDPR's so-called "risk-based approach".

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

Conducting a Data Protection Impact Assessment – checklist I

1. Setting up the project:
   - Compilation of the team: lawyers, technicians, specialized departments, possibly data protection officers, if necessary external consultants
     - Time and resource planning
     - Commitment of the management
2. Describe the planned processing including their purposes
3. Obtaining the views of the data subjects or their representatives
   - Obligation if such a position exists or is foreseeable
   - Implies the information of those affected
4. Evaluate the necessity and proportionality



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

LAW AND INTERNET FOUNDATION

LATVIAN ASSOCIATION OF LOCAL AND REGIONAL GOVERNMENTS

SMA THE EXTENDED ENTERPRISE

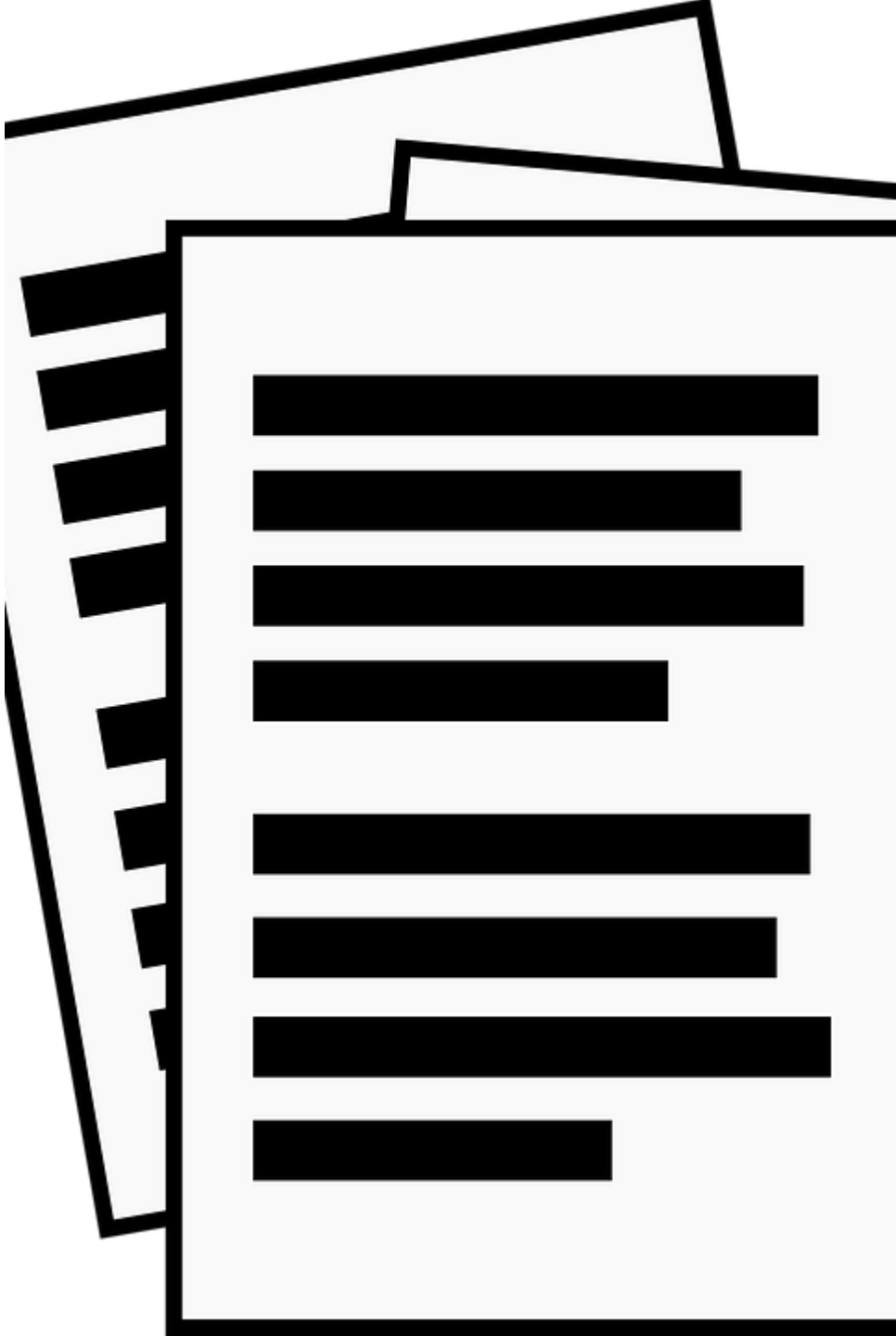
Conducting a Data Protection Impact Assessment – checklist II

5. Identify and evaluate the risks for those affected:
   - Probability
   - Consequences of risk realization
   - The product of these two factors is the final risk value
6. Taking measures to deal with the risks
7. Documentation of the Data Protection Impact Assessment (Report) with evidence of compliance with the requirements of the GDPR
8. Ongoing verification/assessment that the assumptions and forecasts made in the Privacy Impact Assessment were correct and that the processing was carried out in accordance with the DPIA specifications

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

Documentation: Report of DPIA

- Recommended: accompanying the DPIA process with documentation in the sense of a "living document“.
- 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.
- GDPR does not provide for any specific rules for the design of a DPIA report nor for the process to for conducting a DPIA.
- criteria listed by the Article 29 Data Protection Working Party in Annex 2 of WP 248, essentially based on Article 35, para 7 GDPR.
- 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



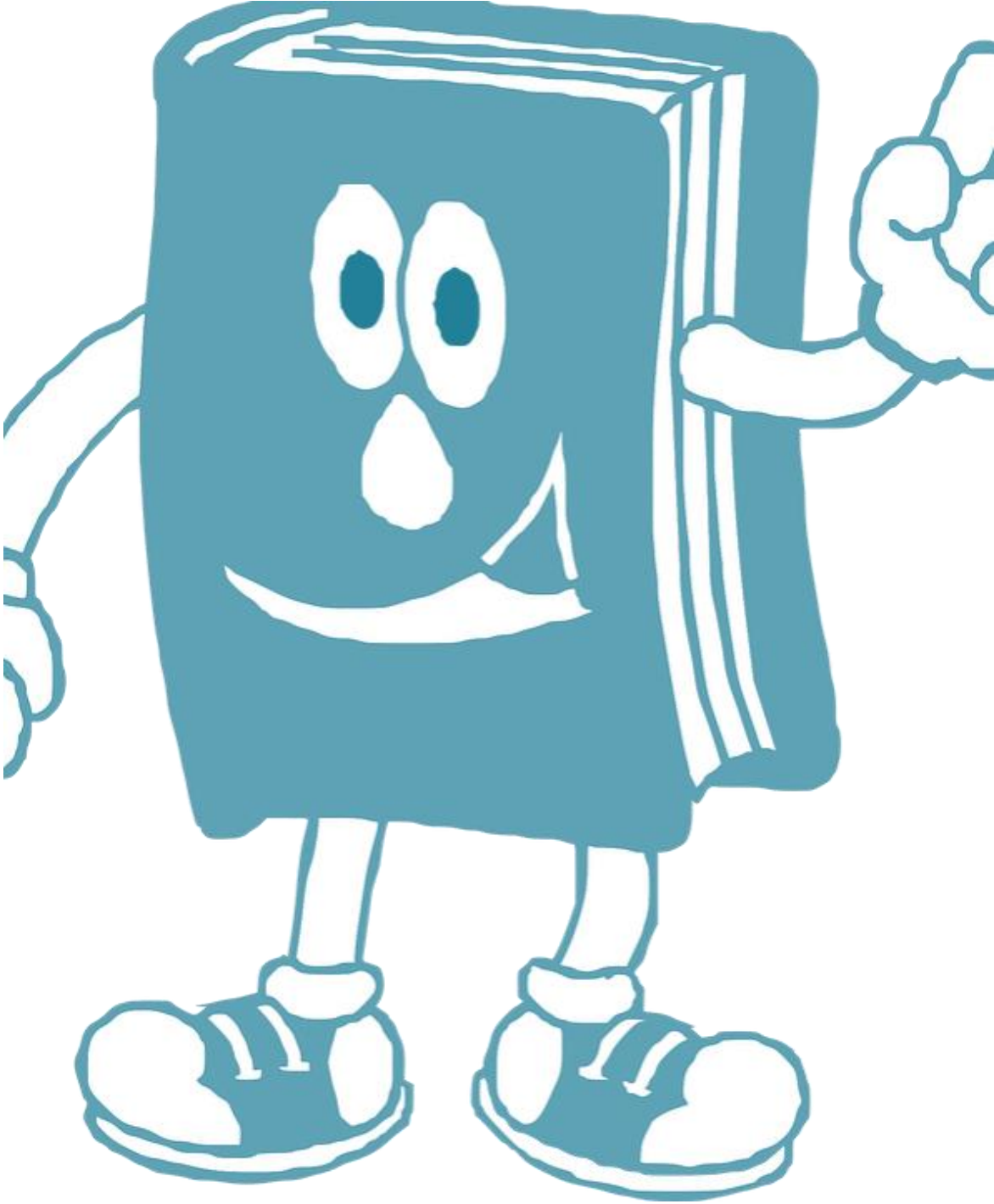
Recomendations & insentives

- Documentation of all decisions, in particular why, if necessary, no data protection impact assessment was carried out.
- In case of doubt, carry out a data protection impact assessment.
- Inclusion of internal and external stakeholders.
- Use of examples, best practices, and, if appropriate, similar DPIAs already in place.
- 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.
- Publish the DPIA
  - In particular by public authorities
  - Shows privacy awareness and builds trust

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

Suggestions for further reading:

- Art. 29 Working Group, WP 248: 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
- Germany: Forum Privatheit White Paper DSFA: https://www.forum-privatheit.de/forum-privatheit-de/publikationen-und-downloads/veroeffentlichungen-des-forums/themenpapiere-white-paper/Forum-Privatheit-WP-DSFA-3-Auflage-2017-11-29.pdf
- CNIL, The open source PIA software: https://www.cnil.fr/en/open-source-pia-software-helps-carry-out-data-protection-impact-assesment
- Privacyofficers.at, https://www.privacyofficers.at/privacyofficers-at-veroeffentlicht-beispiel-zur-durchfuehrung-einer-datenschutz-folgenabschaetzung/
- Paul Voigt, Axel von dem Bussche, The EU General Data Protection Regulation (GDPR): A Practical Guide, 2017



Transparency

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

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 Working Party 29, transparency is aimed at empowering data subjects to hold data controllers and processors accountable and to exercise control over their personal data.
- 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.

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

Elements of transparency under GDPR

“Concise, transparent, intelligible and easily accessible”

- The first two parts of this requirement mean that data controllers should present the information 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.

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

“Concise, transparent, intelligible and easily accessible”

- 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.
- It is advisable 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.
- 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.

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

“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. 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.
- 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.

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

Free of charge provision of information

- 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* (*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.

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

Information to be provided to the data subjects

What information should be provided?

The GDPR outlines 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:

- information about their identity, including their contact information;
- contact details of the Data Protection Officer;
- purposes of processing and their foundation in law – mostly for local authorities the foundation would be the exercise of official authority vested in the controller, and the respective provisions of the national legislation;
- the type of data that is processed, when it was not provided by the data subject;
- 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.

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

What additional information should be provided?

- the period for which the personal data will be stored, or the criteria used to determine that period;
- 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;
- where the processing is based on consent, the existence of the right to withdraw consent at any time;
- the right to lodge a complaint with a supervisory authority;
- the existence of automated decision-making, including profiling, and meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

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

What additional information should be provided?

- 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 mandatory requirement.
- 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 initially. 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.

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

How the information should be provided?

- The default way of providing information to and communicating with data subjects is in writing.
- GDPR also permits information to be provided by other means, including electronic.
- Information may be provided orally to a data subject on request, if their identity information is proven by other (i.e. non-oral) means.

How the information should be provided?

- 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. 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.

- In cases of oral provision of information, data controllers should still be able to demonstrate that they complied with the GDPR's requirements. They should ensure that they have a record of:
  - the request for the information by oral means;
  - the method by which the data subject's identity was verified; and
  - the fact that information was provided to the data subject.

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

When to provide information?

- Information about the processing of personal data should be given to the data subject at the time of the collection;
- 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;
  - second, if is expected that the data will be disclosed to another recipient, at the latest at the first disclosure to that recipient.

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

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

- When 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. 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. WP29 recommends reminding data subjects of the scope of data processing on a regular basis.
- 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.

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

Modalities

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

Privacy notices & statements

- In an online environment it is recommended to use 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.
- 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.

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

“Push” & “pull” notices

- A pull notice required the website users to look for information, in particular information on data processing:
  - Example: “learn more” button where the user can manage privacy settings.
- A push notice is brought to the attention of the user without any actions on their side:
  - Example: “just-in-time” notice provides 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 a certain online service after filling a form. Before the citizen files the form, such just-in-time notice may appear.

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

Other types of “Appropriate measures”

Outside the digital environment, appropriate measures 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.

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.

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

Visualisation

- 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.

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 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.).

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

Exemptions of the obligation to provide information

- When the request is manifestly unfounded or excessive, in particular because of its repetitive character, in which case the data controller may refuse to act on it altogether, instead of charging the data subject a reasonable fee. The controller must prove the manifestly unfounded or excessive character of the request. It should also inform the data subject of the reasons for its decision without undue delay and at the latest within 1 month after receiving the request. The refusal must contain information about the possibility of lodging a complaint with a Supervisory Authority and seeking judicial remedy.
- When the controller has reasonable doubts about the data subject's identity. In this case controllers can require additional information necessary to confirm the identity of the data subject and ultimately, they can refuse access to information.

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

Exemptions of the obligation to provide information

- The third exception concerns information under *Art. 13 and 14*. In certain cases, local authorities are exempted from the obligation to provide this information. When the data are acquired from the data subject, the only such case is when he or she already has the information;
- When the data are not obtained from the subject, the exceptions are more:
  - 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 national 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 EU or national law, including a statutory obligation of secrecy; this exception may be applicable to autonomous municipal companies and similar entities.

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

Conclusion

- 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.

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

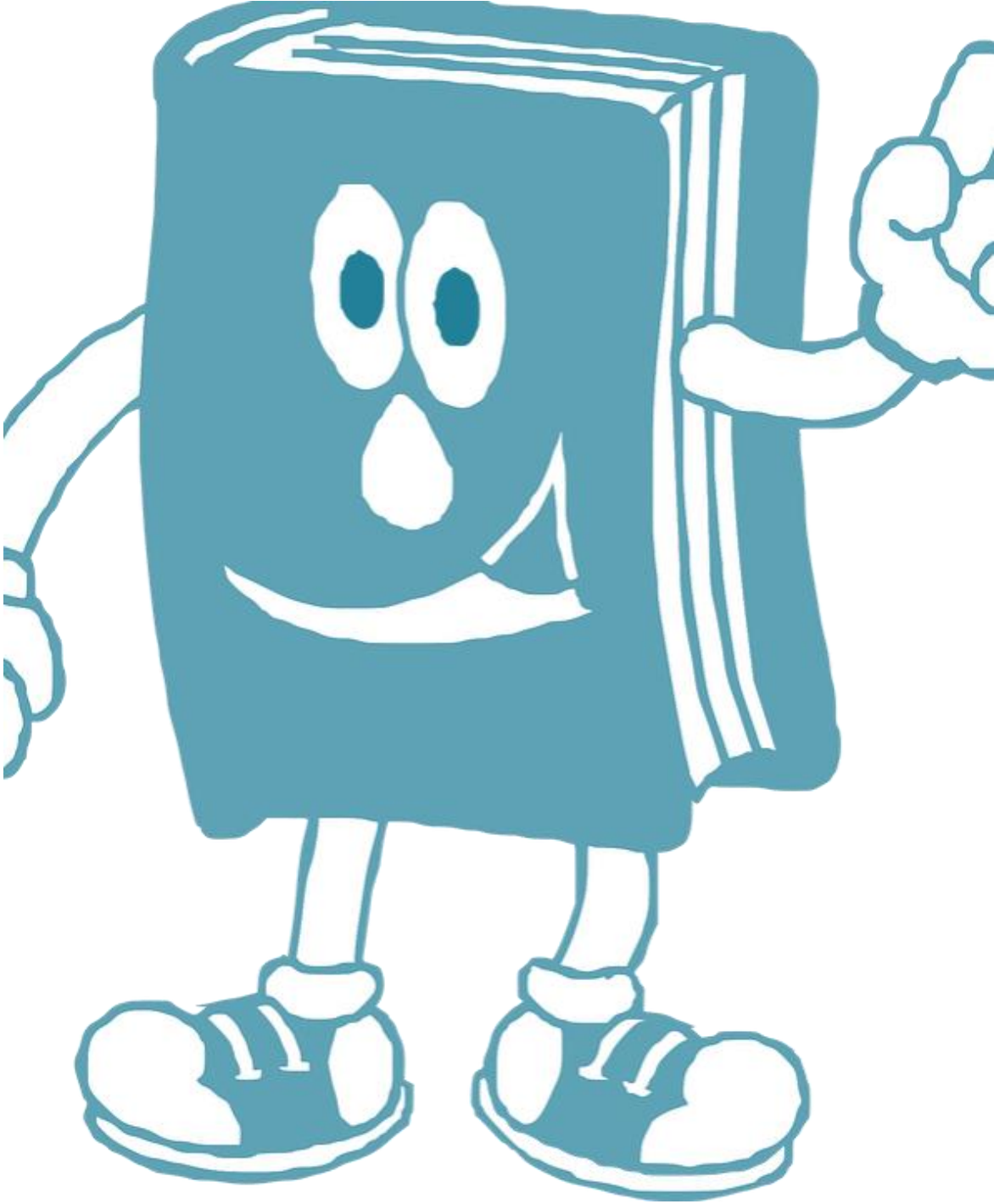
Conclusion

- 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 example, they can put up information posters in their public offices and distribute leaflets encompassing the information;
- 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;
- 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 correctly.

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

Suggestions for further reading:

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



Disclosure of information
or
Right of access by the data subject
Article 15 GDPR

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

LAW AND INTERNET FOUNDATION

LATVIAN ASSOCIATION OF LOCAL AND REGIONAL GOVERNMENTS

SMA THE EXTENDED ENTERPRISE

SNSPA

Right of Access: Legal framework

- **Article 15:** Right of access by the data subject
- **Recital 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…
- **Recital 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…

Right of Access: function and purpose

- The purpose of this right: 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 rectification or erasure) or the lawfulness of the processing.

- **Right to access is a central institution of data protection legislation**
  - basis for the data subject to exercise any other rights.
  - controllers should be well prepared for this process.

- The **best preparation** are well structured and best possible detailed **records of processing** activities.

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

Right of access entitled to the data subjects

1. The right to ask the controller to confirm **whether or not personal data** of the requesting subject **is being processed,**
   - ➢ also "negative information“, if no data are processed.

2. The **right to obtain a copy of the personal data,**
   - ➢ additional copies my be charged with reasonable fee;
   - ➢ application electronically → common electronic format.

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

Article 15 (1) GDPR
Right of access by the data subject

The data subject has 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;

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

Article 15 (1) GDPR
Right of access by the data subject

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.

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

Content of information - overview

Art 15 Para 1 GDPR	Conten of the information
lit a	the purpose of processing
lit b	categories of personal data processed
lit 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
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.

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

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

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

- **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.
- Controller **has to inform data subject** about the extension of the deadline:
  - within one month after receiving the request;
  - together with the reasons for the delay; and
  - information of the possibility to lodge a complaint.
- **Attention!** All communications must be **in a clear and simple language** in a precise, transparent, understandable and easily accessible form.

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

Form of application and answer

- **No compulsory form**, the request for information can be made orally, in writing or in digital form (e.g. e-mail).
- Reply in any **appropriate form**, but to be observed:
  - written request is best answered in writing;
  - common method: submitting a copy of an identity document (official ID) to the application → answer as registered mail to the person.
- If required by the applicant: orally, **provided that the identity of the data subject has been established** in another form.
- If the data subject submits the **application electronically**
  - information provided in a common electronic format;
  - If possible, the controller may also provide remote access to a secure system for data subjects direct access to their personal information.

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

Obligation to proof the applicants identity as the data subject

- **Identity of the** person requesting (the **applicant**) **must be clear**
  - ➢ the controller may request additional information if he/ she has "reasonable doubt" about the identity of the applicant (Art. 12 para 6).
- Recital 64: the controller should use **all reasonable means to verify the identity of the applicant** → particularly in online services;
- Identity authentication **to ensure data security appropriate to the risk of data breach**, if the data is transmitted to the wrong recipient.

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

LAW AND INTERNET FOUNDATION

LATVIAN ASSOCIATION OF LOCAL AND REGIONAL GOVERNMENTS

SMA THE EXTENDED ENTERPRISE

SNSPA

Reimbursement of costs for the access

The access to information is to be provided free of charge (Art 12 para. 5 GDPR).

- In the case of manifestly unfounded or excessive (particular in the case of frequent repeatedly) 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.

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

LAW AND INTERNET FOUNDATION

LATVIAN ASSOCIATION OF LOCAL AND REGIONAL GOVERNMENTS

SMA THE EXTENDED ENTERPRISE

SNSPA

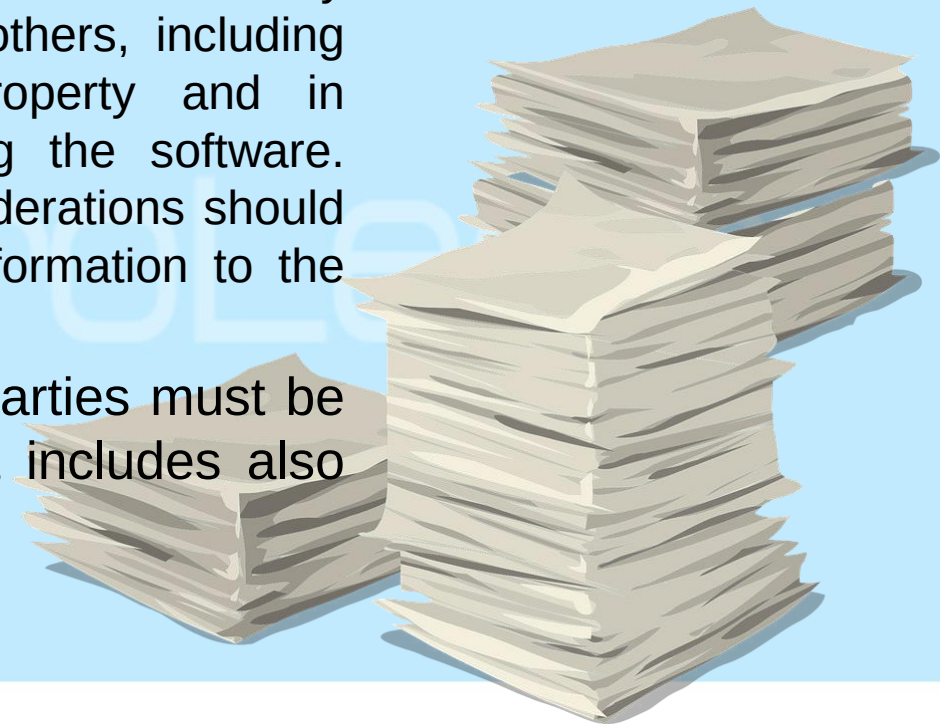
Obligation of the applicant to participate

- Such obligation is not explicitly stated in GDPR, but could be derived from Recital 63:
  - acknowledge in the literature throughout the EU;
  - also recognised in Austria by the Data Protection Authority and the under the previous data protection act (DSG 2000): “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**.”

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

Rights of third parties when disclosing information to the data subject

- Article 15 (4) GDPR: **right to receive a copy may not affect the rights and freedoms of others**
  - Also Recital 63: “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.”
- Basic rule: personal data of third parties must be deleted from the data copy – that includes also business/professional secrets.



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

Checklist for disclosing information on request

Am I obliged to provide information?

- E.g. an organisation is merely a processor, but still receives a request, it must immediately forward it to the person responsible.

Identity check

- If in doubt about the identity: Request proof from the applicant

Is there an excessive or manifestly unfounded application?

- e.g. the applicant was often given the same information, possibly cost sharing

Are there personal data of the applicant processed at all?

- If no data has been stored about the applicant → negative information

What data and information does the controller have to provide?

- All data must be provided that is stored from the applicant. Third party rights must be observed

Issuing the information

- The controller has to choose the right channel according to the necessity and method of authenticating the data subjects / applicants identity

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

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

Suggestions for further reading:

- Souhrada-Kirchmayer, The right of access to the DSGVO, in Jahnel [Hrsg], Yearbook 17. Data Protection Law, 2017.
- Martini in Paal/Pauly (Ed.), Datenschutz-Grundverordnung (2016).
- Paul Voigt, Axel von dem Bussche, The EU General Data Protection Regulation (GDPR): A Practical Guide (English), 2017.
- https://www.gdpreu.org/the-regulation/list-of-data-rights/right-of-access/
- The Data Protection Handbook of EU Fundamental Rights Agency (2014): http://fra.europa.eu/en/publication/2014/handbook-european-data-protection-law-2014-edition