INTRODUCTION OF THE DATA PROTECTION REFORM TO THE JUDICIAL SYSTEM
INFORM

JUST-JTRA-EJTR-AG-2016

Action grants to support European judicial training

JUSTICE PROGRAMME

GA No. 763866

INtroduction of the data protection reFORM to the judicial system

INFORM

WP2: Data Protection regulatory review & training material elaboration

D2.4 Review report on GDPR aimed at legal practitioners

Lead partner: Law and Internet Foundation

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission. [1]

Project co-funded by the European Commission within the JUST Programme		
Dissemination Level:		
PU	Public	X
CO	Confidential, only for members of the consortium (including the Commission Services)	
EU-RES	Classified Information: RESTREINT UE (Commission Decision 2005/444/EC)	
EU-CON	Classified Information: CONFIDENTIEL UE (Commission Decision 2005/444/EC)	
EU-SEC	Classified Information: SECRET UE (Commission Decision 2005/444/EC)	
Document version control:		
Version 1	Originated by: Denitsa Kozhuharova, Law and Internet Foundation	09.12.2017
Version 1	Updated by: Svilena Rakshieva, Law and Internet Foundation	20.01.2018
Version 2	Updated by: Dilyana Petkova, Denitsa Kozhuharova, Law and Internet Foundation	12.02.2018
Version 3	Updated by: Desislava Krusteva, Law and Internet Foundation	28.02.2018
Version 4	Updated by: Dilyana Petkova, Denitsa Kozhuharova, Law and Internet Foundation	15.03.2018
Version 5	Revised by: George Dimitrov, Law and Internet Foundation	29.03.2018
Version 5	Reviewed by: Matthias Eichfeld, University of Göttingen	06.04.2018

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

Version 6	Updated by: George Dimitrov, Law and Internet Foundation	13.04.2018
Version 7	Updated by: Desislava Krusteva, Law and Internet Foundation	08.08.2018

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

Executive summary

This document constitutes Deliverable 2.4 Review report on GDPR aimed at Legal Practitioners within INFORM project. It represents a thorough review of the General Data Protection Regulation (GDPR) from the prospective of legal practitioners, who on the one hand, need to know how to construe and apply the Regulation for the purposes of their legal practice and on the other hand – are being themselves in the roles of data controllers, processors or even data subjects.

The document includes 10 Chapters. The first Chapter introduces the rational that lays behind the selection of this particular target group. The second Chapter outlines the material scope of GDPR. Chapter 3 and 4 are one of the key chapters in understanding the whole regulation in the field of personal data protection as it examines its foundations – what personal data is, and how to identify it and what should be considered as processing of personal data.

Chapter 5 examines the figures of data controller and data processor and provides further clarifications on the distinction between them, while Chapter 7 and 9 outline their obligations.

Chapter 6 tackles another major issue in this field of data protection and namely the requirements that should be observed in order to have lawful processing. There is a thorough examination of the concept of consent, which constitutes one of the main legal grounds for processing personal data.

All of the data subjects' rights are carefully examined in Chapter 8. Last but not least Chapter 10 deals with one of the greatest changes in the field of data protection – namely sanctions and liability.

This deliverable also contains an Annex with a comprehensive explanation of the principles of data processing, thus being a valuable part the document. The Annex constitutes unified part of all legal review deliverables within Work Package 2 of the INFORM project and it is prepared in close collaboration between INTHEMIS and UGOE.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

Table of contents

Executive summary 4

Chapter 1: Introduction 10

1.1. Target group 10

1.2. Legal practitioners' relevant activities 11

Chapter 2: Material scope of application of the GDPR with respect to legal practitioners 12

2.1. Processing wholly or partly by automated means or part of a filing system 12

2.2. Exceptions from the material scope 15

2.2.1 Opening clause for specific legislation 16

Chapter 3: The requirement of personal data and its limits 18

3.1. Notion and content, Art. 4 No. 1 18

3.2. Pseudonymisation and Anonymisation, Art. 4 No. 5 24

3.3. Special types of data and the consequences for data processing, Art. 9 26

3.3.1 Genetic data, Art. 4 No. 13 28

3.3.2 Biometric data, Art. 4 No. 14 28

3.3.3 Data concerning health, Art. 4 No. 15 30

Chapter 4: Activities of data processing 33

4.1. Collection 33

4.2. Recording and storage 34

4.3. Use 35

4.4. Dissemination or otherwise making available 35

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

4.5. Other types of processing activities 36
Chapter 5: Who is data controller and who is data processor? 39
5.1. Notion 39
5.1.1. Data Controllers 39
5.1.2. Joint controllers 40
5.1.3 Data processors 42
5.2. Determination based on the definitions in Art. 4, No. 7 and 8 42
5.3. Critical cases regarding the target groups 43
Chapter 6: Lawfulness of processing, Art. 6 ("Rights" of the data controller) 44
6.1. Consent of the data subject 45
6.1.1. Explicit consent 47
6.1.2. The right to withdraw consent 49
6.2. Performance of a contract (Art. 6, para 1, lit. b) 50
6.3. Compliance with a legal obligation (Art. 6, para 1, lit. c) 51
6.4. Protection of the vital interests of the data subject (Art. 6, para 1, lit. d) 52
6.5. Performance of a task in the public interest (Art. 6, para 1, lit. e) 53
6.6. Purposes of the legitimate interest (Art. 6, para 1, lit. f) 54
6.7. Restrictions (of the rights of the data subjects), Art. 23 55
Chapter 7: Obligations of the data controller 56
7.1. Organisational obligations 56
7.1.1. Responsibility of the controller (Art. 24; Recitals 74-79) 57
7.1.2 Record of processing activities, Art. 30 (rec. 82, 89) 60
7.1.3 Security of processing, Art. 32 (rec. 83) 63

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

7.1.4 Privacy Impact Assessment (PIA), Art. 35 (Recitals 84, 90-94) 65

7.1.5. Responsibility of the controller regarding the appointment of data processors (Art. 28, para 1-3, Recital 81) 68

7.1.6 Cooperation with data protection authorities, Art. 31 (Recital 82) 70

7.2. Technical obligations, Art. 25 71

7.2.1 Privacy by design (Art. 25, para 1, Recital 78) 72

7.2.2. Privacy by default (Art. 25, para 2) 75

7.2.3. Certification with indicative effect for legal practitioners (Art. 25, para 3) 77

7.3. The role of the data protection officer 78

7.3.1 DPO's involvement (Art. 38) 83

7.4. Reporting obligations 86

7.4.1 Reporting data breach to DPA, Art. 33 (Recital 73, 85-88) 86

7.4.2. Notifying data breaches to affected data subjects (Art. 34, Recital 73, 86-88) 88

Chapter 8: Awareness and guarantee of the rights of the data subject 89

8.1. Transparent information, communication and modalities for the exercise of the rights of the data subject (Art. 12) 89

8.2. Information to be provided where personal data are collected from the data subject. Information to be provided where personal data have not been obtained from the data subject (Art. 13-14) 91

8.3. Right of access by the data subject, Art. 15 95

8.4. Right to rectification, Art. 16 98

8.5. Right to erasure ("right to be forgotten"), Art. 17 98

8.5.1. Exceptions from the 'right to be forgotten' 99

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

8.6. Right to restriction of processing, Art. 18 101
8.7. Right to data portability, Art. 20 102
8.8. Right to object, Art. 21 104
8.9. Automated individual decision making including profiling, Art. 22 107
Chapter 9: Legal position of the data processor 109
9.1. Indirect obligations, Art. 28, 29 109
9.1.1 Compliance with the controller's instructions, Art. 29 110
9.1.2 Conflicts between controller instructions and applicable law, Art. 28, para. 3 110
9.1.3 Obligation of confidentiality, Art. 28, para. 3 lit. b, Art. 29 111
9.1.4 Appointment of sub-processors, Art. 28, para. 2 and 4 111
9.1.5 Effect of infringement, Art. 28, para. 10 112
9.2. Direct obligations 113
9.2.1. Accountability, Art. 30, para. 2 113
9.2.2. Data Security, Art. 32, para. 1 115
Chapter 10: Sanctions and liability 118
10.1. Remedies available to data subjects 118
10.1.1. Right to lodge a complaint with a supervisory authority, Art. 77 118
10.1.2. Right to an effective judicial remedy against a supervisory authority, Art. 78, para 1 and para 2 119
10.1.3. Right to an effective judicial remedy against a controller or processor, Art. 79 120
10.1.4. Right to representation by not-for-profit body, organisation or association, Art. 80 120
10.2. Liability of data controllers and data processors 122
11. Conclusion 127

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

ANNEX 128

Fundamental principles relating to processing of personal data 128

1. Principles of lawfulness, fairness, transparency 129

1.1. Lawfulness 129

1.2. Fairness 130

1.3. Transparency 131

2. Principle of purpose limitation 132

2.1. Specified purpose 132

2.2. Explicit purpose 133

2.3. Legitimate purpose 134

2.4. Compatible use 134

3. Principle of data minimisation 139

5. Principle of storage time limitation 140

6. Principle of integrity and confidentiality 141

7. Accountability 141

7.1 Liability of the data controller or data processor 142

7.2 Accountability and data protection by design and by default 142

8. Prohibition of automated decision-making 143

Bibliography 145

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

Chapter 1: Introduction

The current document is developed under Work Package 2 of the INFORM project. The aim of this report is to review the new data protection legal requirements, introduced by Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation, here and after referred to as GDPR). The report is a product of an in-depth review of the GDPR with regard to its application and interpretation by one of the INFORM main target groups - "legal practitioners". At the same time, the report will also tackle how and whether legal practitioners should comply with GDPR requirements in their role as data controllers and data processors[1].

1.1. Target group

The results of the analytical activities demonstrated in this document aim to benefit legal practitioners by clarifying on the one hand their own rights and obligations under the GDPR, and on the other hand, by providing guidelines how to construe the provisions of the Regulation in their daily activities of performing legal services.

For the purposes of this deliverable, the term "legal practitioners" encompasses any person, who pursues a legal profession, and is not a part of the judiciary. This includes, but is not limited to lawyers, legal advisors, bailiffs, notaries, barristers, attorneys, solicitors, etc. The broad scope of the definition aims to overcome different meanings and acceptations of the terms in the jurisdictions throughout the European Union (EU). Moreover, the current report aims to generalise the target group in terms of their legal practice – regardless of the domain they are active in (i.e. commercial law, family law, etc.) or whether they provide legal service in consultancy or litigation.

[1] The terms used in the current report are given thorough definition and explanation in Deliverable 2.11 Data Protection Glossary elaborated under the INFORM project.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

1.2. Legal practitioners' relevant activities

The purpose of outlining the relevant activities of the target group is to contextualise the analysis of the GDPR that follows in view of the diversity of personal data processing activities and to draw attention to the different applications of the GDPR. The report aims to provide a general illustration of the scope of activities, which should be compliant with GDPR. However, the current document provides only an exemplary overview of some distinctive activities with the goal to create a situational context and thus the list of activities should not be considered exhaustive.

At minimum, the following categories of activities should be taken into account:

- Processing of personal data for operational purposes within the organisation they are affiliated to, including but not limited to:
    - Processing of personal data of clients;
    - Processing personal data related to cases;
- Cases on personal data processing.

The first category relates to personal data that is exchanged within the organisation that the legal practitioner is affiliated to – from information gathered for recruitment purposes to information of the contacts of the water delivery service company. Such types of information are processed by any legal entity regardless of their operational field. The activity „Processing personal data of clients" is in practice a subsection of the aforementioned category, as legal offices maintain and store this data, as a critical part of the performance of their professional activities. Another closely related subsection is the personal data related to or within cases. This information is quite sensitive, as it is also protected by the legal professional privilege[2]. The legal professional privilege bounds the legal practitioner not to disclose to third parties the information shared by a client.

The second important group of activities related to personal data processing are the situations where a legal practitioner is dealing with a case on personal data protection issues. This could be cases where

[2] I.e. Case C-550/07 P Akzo Nobel Chemicals Ltd and Akcros Chemicals Ltd v European Commission.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

the main object of the issue is related to data protection violation, or even cases where this object has a minor role. The latter may turn out to be of huge importance to secure the timely and adequate exercise of the data subject's rights and obligation under the GDPR, therefore all legal practitioners should be aware of the GDPR provisions and fields of application regardless of their field of expertise.

Chapter 2: Material scope of application of the GDPR with respect to legal practitioners

This chapter aims to analyse the way legal practitioners should perceive the provisions enshrined in GDPR.

2.1. Processing wholly or partly by automated means or part of a filing system

Pursuant to Art. 2, para. 1 GDPR, the Regulation applies to the processing of personal data wholly or partly by automated means (such as processing through a computerised system or database); as well as to the processing of personal data by other (non-automated) means that form part or are intended to form part of a filing system.

The wording of this provision essentially remains unchanged from the definition of the material scope provided by Art. 3, para. 1 of the Data Protection Directive. It goes in line with and strengthens the legislator's intent to cover all possible techniques of processing, thus preventing the evasion of certain types of data out of the material scope of the European data protection legislation. In practice, the terms of Art. 2, para. 1 GDPR indicate that the Regulation virtually applies to all kinds of processing of data – automated, partly automated and manual.

In order to ensure this broad coverage and to avoid risks of circumvention, Recital 15 GDPR states that *"the protection of natural persons should be technologically neutral and should not depend on the techniques used"*. This text refers to the principle of technology neutrality which, in the context of processing of personal data, applies mainly to the processing of data through automated means (i.e. through technology).

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

Examples of processing through automated means include processing through the use of computers, smartphones, webcams, dashcams, camera drones, as well as through wearables and other smart and IoT devices.[3]

Although there is no specific definition of the term "technology neutrality", it is of a widespread understanding that it is built upon at least two elements, namely: rules should be equally applicable online and offline, and they should not discriminate against a particular technology.[4] Clear from the terms of Recital 15 GDPR the legislator strives to impose the respect of technology neutrality which is often quoted as *the guiding principle for proper regulation*.[5] Abiding by this principle would ensure that no technology, either commonly used, currently in development, or even not yet invented, escapes from data protection regulations. As a result, the provisions of Art. 2, para. 1 GDPR are able to secure a very broad interpretation of the material scope of application of the Regulation and thus guarantee a high level of protection to data subjects.

Further to the processing of personal data through automated means (and the principle of technology neutrality applicable thereto), Recital 15 GDPR clarifies that the protection of natural persons should apply *"to manual processing, if the personal data are contained or are intended to be contained in a filing system. Files or sets of files, as well as their cover pages, which are not structured according to specific criteria should not fall within the scope of this Regulation."*

With view to the above, manual processing which, as opposed to automated processing, is executed exclusively by humans, falls under the provisions of the GDPR in case the following conditions are met:

(1) Data must be contained or intended to be contained in a filing system – Pursuant to Art. 4, No. 6 *"'filing system' means any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis"*. According to the

[3] Voigt P., von dem Bussche A., *The EU general data protection regulation (GDPR). A practical guide*, Springer International Publishing, 2017, p. 10
[4] Reed C., *"Taking Sides on Technology Neutrality"*, 2007, 4(3) SCRIPT-ed 264, p. 264
[5] Ibid., p. 266

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

guidance provided by the UK's ICO[6] *"information stored in a systematic way, but not held in traditional manila files in a conventional filing cabinet or wall-mounted file hangers, may still be held in a 'filing system' if the system is structured to allow easy access to specific information about individuals"*.[7] In addition, while a filing system is generally associated with paper documents, it may as well contain other records, such as microfiche records.[8] The filing system does not need to comprise many files – as long as there is a record structure, it will fall under the GDPR provisions.

(2) Data must be structured according to specific criteria – The GDPR provisions do not provide any requirements on what these criteria should be. Prior legislation, academic research and Court of Justice of the European Union (CJEU) case law demonstrate that such criteria may include chronically organised files, alphabetically organised files or files organised according to other pre-determined criteria.[9] For instance, it has been found by Advocate General Kokott in her Opinion in Case C-434/16 that the concept of a "filing system" covers *"any structured set of personal data which is accessible according to specific criteria. A physical set of examination scripts in paper form ordered alphabetically or according to other criteria meets those requirements."*[10] In addition, the filing system does not need to comprise many files – as long as there is a record structure, it will fall under the GDPR provisions.[11]

Different kinds of folder systems, which are used in most law firms and consist of documents pertaining to different cases and clients, whether on paper, on a server or on a cloud service, fall without a doubt within the definition of "filing system" under the GDPR.

In conclusion, while assessing the processing of personal data through automated means, a special attention shall be paid to the principle of technology neutrality which strives to guarantee that

[6] Information Commissioner's Office (ICO) is the UK's independent body set up to uphold information rights. ICO official website accessible on https://ico.org.uk/
[7] ICO Guide, *"Determining what information is 'data' for the purposes of the DPA"*, available on https://ico.org.uk/media/for-organisations/documents/1609/what_is_data_for_the_purposes_of_the_dpa.pdf
[8] Ibid., p. 6
[9] Voigt P.,von dem Bussche A., *op. cit.*
[10] Opinion of Advocate General Kokott, delivered on 20 July 2017 in Case C-434/16, *Peter Nowak v Data Protection Commissioner*, Rec. 69
[11] ICO Guide, *op. cit.*

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

legislation (incl. its interpretation) should focus on the effects and not the means of a given processing technology. While, on the other hand, when processing of personal data through means other than automated is examined, what is relevant is the existence of a structure established according to certain criteria.

2.2. Exceptions from the material scope

Paragraph 2 of Art. 2 introduces several exceptions from the material scope of the Regulation. In accordance to Paragraph 2, lit. a in liaison with Recital 16, the Regulation shall not apply to issues related to activities which fall outside the scope of Union law, such as activities concerning national security. Similar to this one is the exception related to processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security, Art. 2, para. 2 lit. d. The latter is regulated by Directive 2016/680[12] known as Police Directive, which is *lex specialis* to the GDPR. In Recital 14 of the Directive it is explicitly stated that it "*should not apply to the processing of personal data in the course of an activity which falls outside the scope of Union law, activities concerning national security, activities of agencies or units dealing with national security issues*". However, these entities are obliged to comply with GDPR when performing activities, which are not by their nature excluded from the material scope of the Regulation, such as processing data for operational needs – processing data of their staff (i.e. in relation to employment), partners (i.e. in relation to service contracts) and so on. So here, it is essentially important to provide guidance to such structures on the matter which of their activities fall out of the scope of the Regulation and which do not. Legal practitioners are excluded from the scope of the Directive, as they do not fall within the definition of "competent authority" under Art. 3, para. 7.

[12] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

Example: A Law Enforcement Authority decides to integrate a new automated system for face recognition. In order to assess the efficiency of the new system the testing involves scanning and analysing video records, which constitute evidences to already solved cases. In this case, the applicable law is GDPR, as the processing of personal data does not pursue the specific aims set in the Directive – prevention, investigation, detection and prosecution of criminal offences, rather the processing is needed to test how accurate and efficient the new system is.

2.2.1 Opening clause for specific legislation

The so called "opening clauses" in GDPR provide Member States with discretion of adopting specific national legislative measures to complement the application of the GDPR. It should be taken into account that those "measures", as stated in Recital 41, may not "*require a legislative act adopted by a parliament, without prejudice to requirements pursuant to the constitutional order of the Member State concerned.*" These clauses may confer the right to introduce stricter, less strict or more detailed provisions on national level, which will result in creating complexity in terms of observing the applicable law to a certain case.[13]

From legal practitioners' perspective, one of the key area, where opening clause is envisaged, is in the domain of labour law. Here, various cases may arise from the viewpoint of both employers and employees. Legal practitioners must be aware of the national legislative measures that supplement Article 88 and analyse their compliance with the standards set forth in the Regulation. A useful guideline for applying EU data protection rules within this domain is Opinion 2/2017 on data processing at work adopted by Article 29 Working Party on 8th of June 2017. Another interesting area that will be further detailed will be the processing of the national identification number, see Article 87.

A particularly important aspect of the legal profession is the protection of professional secrecy. The GDPR identifies the processing of data that is subject to professional secrecy as particularly

[13] For instance, Art. 23 envisages that Member States may restrict by way of a legislative measure the scope of the obligations and rights provided for in Articles 12 to 22 and Article 3.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

endangering to natural persons' rights and freedoms (Recital 75, Recital 85). According to Recital 164 of the GDPR, Member States may introduce rules in order to "reconcile the right to the protection of personal data with an obligation of professional secrecy". Further, in Art. 90 the Regulation provides for Member States to adopt specific rules regarding the powers of the national supervisory authorities when controllers/processors obtain or receive personal data in an activity covered by the obligation of professional secrecy. Therefore, legal practitioners should pay close attention to the national legislation in this field.

Key concepts:

Scope of the GDPR: the Regulation is applicable to processing of personal data wholly or partly by automated means, as well as to the processing of personal data by other (non-automated) means that form part or are intended to form part of a filing system.

Automated means: every technology, either commonly used, currently in development, or even not yet invented;

Non-automated means: any means of manual processing, when the data is contained or intended to be contained in a filing system and is structured according to specific criteria.

Exceptions from the material scope of the GDPR: activities which fall outside the scope of Union law, such as activities concerning national security and processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.

Protection of professional secrecy: important under the GDPR and further regulated by national legislation.

Opening clauses – they provide Member States with discretion of adopting specific national legislative measures to complement the application of the GDPR.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

Chapter 3: The requirement of personal data and its limits

One of the key challenges before the application of the data protection legislation is the proper definition of what personal data is and whether a piece of information constitutes in fact personal data. This is of crucial importance for legal practitioners, who need to make legal qualifications on a daily base. In order to address their clients' needs, legal practitioners should be aware of data protection provisions and able to analyse the diversity of cases where their clients should respect the data protection legislation. Therefore, this section analyses the definition of the personal data and its elements.

3.1. Notion and content, Art. 4 No. 1

Art, 4 No. 1 under GDPR introduces the definition of personal data, which should be understood as "*any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person".* This definition is more or less a repetition of the one entrenched in Directive 95/46/EC. However, the new definition outlines in a more detailed, but not exhaustive manner, the scope of what should be regarded as an identifier - name, location data, online identifier. By adding these examples, the European lawmaker left no room for interpretation, as regard these categories. However, one should expect diverse practice in Member States on the scope of the "online identifier", as GDPR does provide broad interpretation of online identifiers in Recital 30 – "*[n]atural persons may be associated with online identifiers provided by their devices, applications, tools and protocols, such as internet protocol addresses, cookie identifiers or other identifiers such as radio frequency identification tags. This may leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them.*"

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

One of the key documents that contains general guidelines on what should be considered as personal data is Opinion 4/2007 on the concept of personal data of Article 29 Working Party[14]. This Opinion clarifies the four elements of personal data:

- "Any information" - according to the Opinion, one must consider as personal data any information regardless of whether it is "objective" or "subjective". This includes "*information regarding whatever types of activity is undertaken by the individual, like that concerning working relations or the economic or social behaviour of the individual. It includes therefore information on individuals, regardless of the position or capacity of those persons (as consumer, patient, employee, customer, etc).*"[15] This information could be available in diverse forms, such as "alphabetical, numerical, graphical, photographical or acoustic" and can have electronic or physical medium.

"The movie star acting as John Snow in the TV show Game of Thrones" – this sentence contains different types of information, which at first glimpse cannot be associated with personal data, however the sentence has enough information to identify who this movie star is, and for every person who knows the TV show and the character, this information is enough to identify the acting star. Therefore, this sentence contains personal data.

- "Relating to" - identifying the relation between information and a particular person is one of the key processes and challenges before the identification of which data is personal. In some cases, the relation is evident – like the address of a person. However, in other situations the relation should be analysed taking into account the specific context in which the information is used. Therefore, Article 29 Working Party outlines three alternative elements of the "relation" that should be present. In Opinion 4/2007 on the concept of personal data is stated that "in order to consider that the data "relate" to an individual, a "content" element OR a "purpose" element OR a "result" element should be present". The "content" relates to the most self-evident cases, where no purpose or impact needs to be analysed in order to define whether the information is personal. "The "purpose" element can be considered to exist when the data are used or are likely to be used, taking into account all the circumstances

[14] Article 29 Working party, Opinion 4/2007 on the concept of personal data, WP136
[15] Ibid.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

surrounding the precise case, with the purpose to evaluate, treat in a certain way or influence the status or behaviour of an individual." In cases where, no purpose or content can be analysed, the "result" should be considered – "data can be considered to "relate" to an individual because their use is likely to have an impact on a certain person's rights and interests, taking into account all the circumstances surrounding the precise case".

In the provided example, the information "John Snow", "movie star", "Game of Thrones" relates to the person Christopher Catesby "Kit" Harington.

- "Identified or identifiable". The next element of the definition that needs an examination are the concepts of "identified or identifiable". The terms "identified" and "identifiable" are key notions which reveal that personal data refers not only to information which allows for the identification of a natural person but also to information which allows for the *possibility* for such identification, or for the so-called identifiability. A person is "identified", when "*he or she is "distinguished" from all other members of the group*"[16], while a person is "identifiable" when there is a possibility to be identified and thus distinguished from all other members of a group. What should be noted here, is the notion of "direct or indirect" identifiability. Yet again, when analysing whether a person can be identified directly or indirectly one should consider the circumstances of a particular case. For instance, in general a person can be identified directly by his/her first name in a small group of people, but not in a large group[17]. In the latter case, additional information is needed in order for the person to be identified. The combination of this information enables the identification.

Generally speaking, and pursuant to the meaning of the suffix *-able*, a person is identifiable when he or she has not yet been identified but there is a possibility for him or her to be identified. In practice, the term "identifiable" opens room to interpretation and allows for various types of information to fall within the scope of the notion "personal data" and thus to be covered by the European personal data legislation.

[16] Ibid.
[17] I.e. in a small group, there is one George or one Mary, but a larger group chances are the more individuals will bear these names, thus making the identification of a certain George and Mary impossible.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

In the mentioned example, the information "movie star" is not enough to identify a person. Movie star acting in Game of Thrones is also insufficient to single out one person. However, by adding the additional information about the character "John Snow" the combination of this information is enough to identify the particular person.

Pursuant to the terms of the former Data Protection Directive and more precisely of its Recital 26 *"to determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person"*. The "reasonable likeliness of identifiability" is a concept which is largely open to interpretation and has raised issues as to how the assessment shall be carried out. According to some authors[18] the topic was widely debated in doctrine[19] due to a high controversy rooted in the argument whether the reasonable likeliness of identifiability shall be established using absolute criteria or using relative criteria. According to the doctrine, in the first case scenario, i.e. where the identifiability is established thought an absolute criterion, the definition of personal data is met as soon as there is any possibility of linking given information to a certain individual. On the contrary, the identifiability would be relative in case it allows for identifying certain individual, thus for rendering data personal, through a proportionate effort in terms of time, cost and manpower.

- "Natural person" – the Regulation only applies to living human beings. This corollary is based on the principles of civil law – the deceased are not subjects to law. This notion is enshrined also in Recital 27 of GDPR stating that – "*[t]his Regulation does not apply to the personal data of deceased persons. Member States may provide for rules regarding the processing of personal data of deceased persons*".

Critical cases in this regard

In October 2016 CJEU provided some very useful and much needed guidance on the matter. In its judgment in Case C-582/14, *Patrick Breyer v Bundesrepublik Deutschland*, the CJEU ruled that the dynamic internet protocol (IP) address of a visitor constitutes personal data if the operator of the website has

[18] Voigt P. and von dem Bussche A., *"The EU General Data Protection Regulation (GDPR). A Practical Guide"*, Springer International Publishing AG 2017
[19] Voigt P., *Datenschutz bei Google*, MMR, 2009, pp. 377-382; Bergt M, *Die Bestimmbarkeit als Grundproblem des Datenschutzrechts – Überblick über den Theorienstreit und Lösungsvorschlag*, 2015, pp. 365-371

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

the legal means allowing for the identification of that visitor with the help of some additional information about him which is held by the internet access provider.

The triggering point was the action brought before the German jurisdictions by Mr Patrick Breyer who sought an injunction to prevent the websites administrated by the Federal institutions, which he visited, from storing his IP addresses. The case went up to the Bundesgerichtshof (the German Federal Court of Justice) which made a reference for a preliminary ruling to the CJEU asking *"whether an IP address which is used to access a web page constitutes personal data for the public authority owner of that page, where the Internet service provider has the additional knowledge required in order to identify the data subject"*. In essence, the CJEU had to rule on whether, as regards the provider of the web page, the dynamic IP address should be classified as personal data in cases where a third party has additional data which, combined with the IP address, identify persons who access its pages; i.e. under what circumstances, a data subject can be found identifiable.

In its Opinion[20] on the Case, the Advocate General Campos Sanchez-Bordona reminded the intense doctrinal debate in Germany which has polarized academic and judiciary opinions dividing them on the question whether criteria, used to assess identifiability, should be objective (absolute) or subjective (relative). According to the theory of the absolute criterion, says the Advocate General, a user is identifiable, and the IP address should be considered personal data, when, regardless of the abilities and means of the provider of an online service, it is possible to identify a certain individual by combining that dynamic IP address with data provided by a third party (e.g. an Internet service provider). On the opposite side, for the supporters of the relative criterion theory, the mere possibility that an individual may ultimately be identified with the assistance of a third party does not automatically make him identifiable and is thus insufficient for a dynamic IP address to be classified as personal data. What would be relevant in this case, explains the Advocate General, is the capacity of the holder of a certain data to use a certain amount of resources to identify an individual from those data.

[20] Opinion of Advocate General Campos Sanchez-Bordona, delivered on 12 May 2016 in Case C-582/14, *Patrick Breyer v Bundesrepublik Deutschland*

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

In its Opinion Advocate General Campos Sanchez-Bordona emphasised on the wording of Recital 26 of the Directive and suggested that a person is identifiable when the means, used by the controller assisted by a third party, to identify that person, are likely *reasonably* to use.[21] This would not be the case where these means are very costly in human and economic terms, or practically impossible or prohibited by law. The Court followed this understanding and held that, in order for a certain data subject to be identifiable, the means likely reasonably to be used to identify him or her should not be prohibited by law or practically impossible on account of a disproportionate effort in terms of time, cost and manpower.[22] Therefore, the identifiability of the data subject is, according to the Court, established through relative criteria.

The CJEU judgement paved the way towards a clearer understanding of how the identifiability should be interpreted. The GDPR recognises the relativity of data subject's identification. Its Recital 26 explains that in order to ascertain *"whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments."*

The CJEU decision and the wording of Recital 26 GDPR provide useful practical guidance as to how to interpret and rule on the identifiability of a data subject should a case involving such issue arise before national judges and law practitioners. When addressing the identifiability, every case should be considered individually taking into account all objective factors, including the following:

- The costs of the identification;
- The amount of time required for the identification;
- The available technology at the time of the processing;
- The technological developments at the time of the processing;
- The manpower / efforts required for the identification;

[21] *Ibid*, Rec. 68
[22] See Rec. 46 of the judgment

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

- The relevant national and EU legal framework allowing for (or eventually prohibiting) the identification;
- The purpose of the processing.

Exercising the legal profession will always inflict processing personal data of clients and other subjects such as other participants in legal proceedings, the other parties to a contract etc. Legal practitioners should keep in mind that this data is protected by professional secrecy and is also under the special protection of GDPR[23].

3.2. Pseudonymisation and Anonymisation, Art. 4 No. 5

Pseudonymisation and Anonymization are both techniques which constitute security measures to ensure a high level of data protection. Legal practitioners should recognise the differences between these techniques, as to provide expert guidance to their clients on the business processes they maintain and design, and the necessity to comply with the GDPR requirements, while in certain cases of anonymisation, the GDPR is not applicable.

First of all, it should be noted that both pseudonymisation and anonymization constitute further processing of information, e.g. a type of processing. These types of processing activities have been analysed by Article 29 Working Party in their opinions[24].

The definition of anonymisation may be extracted from Recital 26, which outlines the anonymous data as "*information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable*". By definition, in order to have anonymised data, the anonymisation process should not be reversible, e.g. the re-identification of the data subject should not be possible. There are different anonymisation techniques, however, Article 29 Working Party recognises two general approaches to anonymisation. This view has been shared by

[23] For more information, see p. 2.2.1 of the current report
[24] I.e. Article 29 Working party, Opinion 4/2007 on the concept of personal data, WP136; Article 29 Working Party, Opinion 05/2014 on Anonymisation Techniques WP216

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

the academics[25] as well. In accordance to it, anonymisation techniques can be classified into two categories - *randomization* and *generalization*[26]. The randomisation technique "*alters the veracity of the data in order to remove the strong link between the data and the individual*". Such techniques are noise addition, permutation, differential privacy[27]. Generalisation on the other hand, consists of generalising/diluting the attributes of data subjects by modifying the information to "*extent such that each individual shares the same value*". (i.e., a region rather than a city, a month rather than a week)[28]. Generalisation techniques are aggregation, K-anonymity, L-diversity/T-closeness[29].

What is important to be underlined here is that if an effective anonymisation has been undertaken, e.g. the re-identification is not possible, then GDPR shall not apply to the processing of such anonymised data[30].

A common mistake is to consider as data as anonymised when the name of the person concerned is removed or disguised. For instance, if the original sentence is the following: "Kit Harington acts as John Snow in the TV show Game of Thrones", neither "K.H. acts as John Snow in the TV show Game of Thrones.", nor "XXXX acts as John Snow in the TV show Game of Thrones." is an anonymisation technique, as there is still plenty of information in the sentience, which allows the identification of the person.

Pseudonymisation, on the other hand, is a process of disguising information in such a way that "*the personal data can no longer be attributed to a specific data subject without the use of additional information*"[31]. Therefore, pseudonymisation allows for re-identification and is supposed to be reversible.

[25] Voigt P. and von dem Bussche A., *"The EU General Data Protection Regulation (GDPR). A Practical Guide"*, Springer International Publishing AG 2017
[26] Article 29 Working Party, Opinion 05/2014 on Anonymisation Techniques WP216, p.12
[27] See more Article 29 Working Party, Opinion 05/2014 on Anonymisation Techniques WP216, Opinion 05/2014 on Anonymisation Techniques, p.12-16.
[28] Voigt P. and von dem Bussche A., *"The EU General Data Protection Regulation (GDPR). A Practical Guide"*, Springer International Publishing AG 2017
[29] For more information see Article 29 Working Party, Opinion 05/2014 on Anonymisation Techniques WP216

[30] Rec. 26 – "This Regulation does not therefore concern the processing of such anonymous information, including for statistical or research purposes."
[31] Article 4, No 5 GDPR

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

Pseudonymisation is not a method for anonymisation and the processing of pseudonymised data is regulated by GDPR.

In the definition provided by GDPR on pseudonymisation, a particular attention is paid to storage of the additional information that may allow for the identification of a person. The Regulation requires that this information should be kept *"separately"* and "*is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.*"[32] Legal practitioners should pay particular attention when analysing whether the additional information is kept "separately" as a data controller may be subject to administrative fines if this requirement is not observed.

Article 29 Working party considers encryption as an example of pseudonymisation. However, GDPR mentions encryption alongside to pseudonymisation[33] when outlining possible security measures. Despite this discrepancy in classifying encryption there is no doubt that encrypted data is personal data and should be regulated by GDPR, as it is not really anonymised, since the decryption key makes the encryption of the data reversible. Nowadays, the regulation of this particular security measure is very important as more and more services heavily rely on encryption as a security measure ensuring compliance with personal data protection requirements (i.e. cloud-based services). In most cases cloud service providers should be considered as data processers and as we shall see further in the report, the relation between the data controller and data processor must be based on a contract.

3.3. Special types of data and the consequences for data processing, Art. 9

In Article 9 GDPR introduces several categories of special types of data, so called sensitive data, which are subject to specific provisions. These types of data include personal data "*revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation".* In general, GDPR imposes a prohibition for processing these special types of data. Therefore, legal practitioners should recognise the types of data that fall within

[32] Ibid.
[33] Article 6, No 4 GDPR

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

these categories and the exemptions that allow for processing such kind of personal information. It is of crucial importance as a lot of new business models are based on or include the processing these types of data and data controllers and processors should pay particular attention to this key concept.

The GDPR maintains the obligation to obtain explicit consent in order to process sensitive data, as long as there is no possibility to ignore consent, such as in the following cases:

- When the processing is necessary to comply with employment or social security obligations, provided that it is authorised by EU law, Member State law or a collective agreement;
- When the processing is necessary to protect the life of the data subject, who is not physically or legally capable of giving consent;
- When the processing is carried out by a foundation, association, political party or other non-profit entity with regard to the data of its members;
- When the data subject has made this personal data available to the public;
- When processing is necessary to file a claim or defence in court;
- When the processing is necessary for reasons of public interest, given certain conditions;
- When the processing is necessary for the purposes of preventive or occupational medicine;
- When the processing is necessary for archive, scientific or historic research or statistical purposes.[34]

The Regulation envisages the possibility for Member States to "*introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health*". Therefore, legal practitioners should observe the developments of national legislations in this relation since their clients may be subject to different national regimes. However, according to Recital 53 of the GDPR, these specific national provisions cannot become an obstacle to cross border data processing.

It is important to know from client's perspective, that a company that processes sensitive data on a large scale, including genetic or biometric data, shall (i) carry out data protection impact assessments and (ii) designate a Data Protection Officer in accordance with Articles 35 and 37 of the GDPR.

[34] These are the exclusions from the prohibition in Article 9, Para. 1.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

3.3.1 Genetic data, Art. 4 No. 13

The legal definition of genetic data is provided for in Article 4 No. 13, which should be construed in liaison with Recital 34 of the GDPR. Genetic data is "*personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question*". These analyses can be chromosomal, deoxyribonucleic acid (DNA) or ribonucleic acid (RNA) analysis, or analysis of another element enabling equivalent information to be obtained which allows for unique information.

The inclusion of genetic data under the scope of special categories of data particularly affects the health sector in the context of clinical research activities.

During a civil procedure, the court might decide to order an expert report involving DNA analysis for the purposes of parentage control. The parties are obliged to provide DNA material for the purposes of providing the report. Legal practitioners are allowed to process the results of the report on the basis of art. 9, para.2, lit. f "exercise or defence of legal claims", being the representatives of their clients.

3.3.2 Biometric data, Art. 4 No. 14

With the introduction of the GDPR, biometric data is now explicitly regulated in comparison to the regime established by the preceding Directive 95/46/EC. However, Article 29 Working Party provided in one of its opinions a general guidance on what should be considered as biometric data, namely fingerprints, retinal patterns, facial structure, voices, but also hand geometry, vein patterns or even some deeply ingrained skill or other behavioural characteristic such as handwritten signature, keystrokes, gait, manner of speaking, etc[35].

[35] Article 29 Working party, Opinion 4/2007 on the concept of personal data, WP136, p.8

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

It should be noted that data about a person's physiological or behavioural characteristics only qualifies as biometric data under the GDPR when this data is processed through a specific technical means allowing the unique identification or verification of the identity of a natural person.

A photograph of someone's face only qualifies as 'biometric' in terms of data protection legislation when the photograph is used to either uniquely identify or verify a person's identity. The technologies used for this purpose typically assess a variety of factors (e.g. the distance between one's eyes and nose, nose and mouth, etc.) in order to uniquely identify a person. Ordinary photos of a person thus may not qualify as biometric data but still should be considered personal data.

Example of a case where a photo is to be considered as biometric data:

A trust service provider within the meaning of Regulation 910/2014 hires an IT company to develop face recognition software for new trust service involving personal identification. The IT company creates the software by using photos of natural persons. The applicable legal ground for gathering photos of persons within this case will be the consent of the data subjects. This is also the applicable exception under article 9.

Example of a case where a photo is to be considered only as personal data:

An online media uploads a photo of the champions of the national scientific championship. In this case no exemption under article 9 is needed in order to prove the lawfulness of the processing, as the processing is regulated by Art. 6.

The inclusion of biometric data in the list of special categories of data under Art. 9 of the GDPR will affect almost every company that operates in the information society. This is due to the widely-used authentication mechanisms based on biometric data to identify natural persons, as these mechanisms are the only method of ensuring that a person is who they claim to be. In fact, some companies already control access to private work spaces by employees via fingerprint authentication or by capturing a simple selfie.

One of the security settings of smart phones involves fingerprints recognition to unlock the mobile device. In this case, data subjects consent to the processing of their personal data.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

The qualification of biometric data as a category of 'special data' leads to several consequences for data processors and controllers that were mentioned already. In most of the cases, the latter will need the explicit consent of the data subject concerned to process biometric data, whereas certain organisations in the field of social security or employment, or hospitals, may be able to process biometric data on different legal grounds such as processing for the purposes of preventive or occupational medicine.

Legal practitioners may process biometric data of their employees in restricted cases (such as fingerprint for access to certain documents). The most common practical implication of this aspect of Art. 9 will be for jurists acting in the field of criminal law, which may receive on regular basis biometric data as part of the documentation of different proceedings.

3.3.3 Data concerning health, Art. 4 No. 15

The processing of data concerning health is the third kind of processing of special category of data that could be further regulated by Member States law. In accordance to Art. 4, No. 15 'Data concerning health' means "*personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status*". The legal definition should be interpreted in a broad manner. In 2007 Article 29 Working Party has provided further guidance as to which types of data (beyond the obvious ones such as diagnosis, test results, etc.) are to be regarded as data concerning health[36] - data on drugs/ alcohol consumption, as well as administrative information of admission in a hospital should be treated as data concerning health.

A recruitment procedure in IT company obliges future employees applying for the position of software developer to present medical certificate of having no infections. The request for such information should be considered excessive, and thus unlawful, in such a case for the following reasons: Article 9, para 2, lit b provides for the principle possibility that for the purposes of employment special categories of data can be processed. However, such processing will be allowed if "it is authorised by Union or Member State law or a collective agreement pursuant to

[36] Article 29 Working Party, Working Document on the processing of personal data relating to health in electronic health records (EHR), WP131, p.7.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject.

When assessing whether such a requirement is reasonable, ones must analyse the nature of the position – whether such request is justifiable in the context of the duties that the employee will perform. In this example the request of such information may lead to discrimination and thus the fundamental rights and the interests of the data subject cannot be considered safeguarded. However, if the job profile involves direct access to food (chef in a restaurant), such requirement should not be considered excessive – the nature of the job justifies the adoption of such requirement.

Of particular interest is the case where data concerning health is transferred beyond the national borders of the State where the data was originally collected. In this connection, what is quite important to be considered is that data concerning health could be transferred only when such an action is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent[37]. Article 29 Working Party[38] sheds light as to how this provision should be construed stating that the transfer must relate to the individual interest or to that of another person and must be necessary for an essential diagnosis. Furthermore, Article 29 Working Part has stated that this derogation for transfers of personal data to third countries cannot be used in cases where data concerning health is to be processed for the purposes of performing general medical research.

As employers, legal practitioners should be aware that certain documents of employees, such as medical dossiers, documentation on disability, etc. contain special categories of data, therefore additional measures for protection should be taken towards them. The legal basis for lawful processing in this case is Art. 9, para. 2, lit. b.

[37] Art. 49, para. 1, lit. f, GDPR
[38] Article 29 Working Party, Guidelines on Article 49 of Regulation 2016/679, WP262, p. 4.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

Documents of clients or other parties to legal proceedings may also contain health data, in which case the legal practitioners have legal grounds for processing it (Art. 9, para. 2, lit. f - for the establishment, exercise or defence of legal claims), but nonetheless should be extra careful as regards the security measures and the storage of these data.

From the point of view of legal practitioners, the correct understanding of which types of data are to be regarded as data concerning health is of particular importance when consulting clients in health sector, and likewise when handling cases on data subject's rights violation in terms of unlawful processing of data concerning health.

Key concepts:

Personal data: any information relating to an identified or identifiable natural person ('data subject');

Identifiable natural person: one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Relative identifiability: identifying a certain individual through a proportionate effort in terms of time, cost and manpower.

Pseudonymisation: an operation through which the personal data can no longer be attributed to a specific data subject without the use of additional information.

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

Most important notions for legal practitioners: legal practitioners should recognise the special types of data and the exemptions that allow for processing such kind of personal information. They should also keep up with the national regulations, as Member States are allowed to introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

Chapter 4: Activities of data processing

According to Art. 4, No. 2 GDPR "processing" is any operation or set of operations performed upon personal data or sets of personal data regardless of the means (automated or not) used. Ultimately, any treatment of data is considered "processing". This very broad definition of "processing" reveals the legislator's intention to guarantee that the GDPR provisions apply whenever an organisation does anything which involves or affects personal data. The examples of processing provided by Art. 4, No. 2 include *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*.

The list of examples is not intended to be exhaustive. Processing may cover any conceivable use of data. Processing activities are thus found throughout all operation and business processes of an organisation.

4.1. Collection

Any collection of information from the individual to whom the personal data relates or from a third party is considered "processing" and falls under the scope of the EU data protection regulation.

The collection of personal data may also include gathering information from wearables or other smart devices (smart watches, cars, other IoT devices). The receipt of an e-mail containing information on a natural person is also a collection of personal data.

Taking and storing fingerprints constitutes collection of personal data and is therefore also considered processing. In this sense, the CJEU judgement of 17 October 2013 on case C-291/12, *Michael Schwarz v Stadt Bochum*, confirmed that measures involving national authorities taking a person's fingerprints and keeping these fingerprints in the storage medium in the person's passport must be viewed as a processing of personal data.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

4.2. Recording and storage

Video and voice recording are consistently becoming a more and more frequent form of processing of personal data.

According to an opinion[39] of the Article 29 Working party in cases of telephone banking, where the customer's voice giving instructions to the bank are recorded on tape, those recorded instructions should be considered as personal data; the recording of such data may *ipso facto* be qualified as processing under the meaning of Article 4, No. 2 GDPR. Another example involves images of individuals recorded by a video surveillance system. Such images are considered, according to the opinion of the Working party, as personal data to the extent that the individuals captured are recognizable; therefore, the recording through video surveillance systems shall also be perceived as "processing".

Storage of information, regardless of the means or the subsequent use of this information, is considered as processing of personal data. Storing of information may include the gathering and keeping by a potential employer of job applicants' CVs for future vacant positions. Such storage constitutes processing regardless of whether the data is subsequently used or not.

In this sense is the judgment of the CJEU of 18 February 2004 on Case T-320/02, *Monika Esch-Leonhardt and Others v European Central Bank*, where the Court of first instance of the EU held that *"[w]hen the European Central Bank includes letters concerning the transmission by email of Union information in the personal files of its staff, it is processing personal data by saving them in a personal data filing system."* As the inclusion of those letters in the personal files is in itself capable of adversely affecting the applicants' rights to adequate protection against the unlawful processing of personal data, such storing clearing constitutes processing and shall fall under the provisions of data protection regulations.

[39] Article 29 Working Party, Opinion 4/2007 on the concept of personal data, adopted on 20 June 2007, WP 136

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

4.3. Use

The use of personal data is at the core of the personal data processing activities. In this sense, in its judgement on case C-73/07 the CJEU has reminded that it stems from the wording itself of the definition of Art. 2 (b) of Directive 95/46/EC (currently Art. 4, No. 2 GDPR) that certain activities involving use of personal data should be considered processing. The dispute in the main proceedings involved public tax information collected from documents in the public domain held by the tax authorities and processed for publication, published alphabetically in printed form by income bracket and municipality in the form of comprehensive lists, transferred onward on CD-ROM to be used for commercial purposes, and processed for the purposes of a text-messaging service whereby mobile telephone users can, by sending a text message containing details of an individual's name and municipality of residence to a given number, receive in reply information concerning the earned and unearned income and assets of that person. The Court held that these activities constitute "processing of personal data".[40]

"Use" as a processing activity has a very broad application. For instance, when a lawyer communicates with its clients by sending them emails or calling them – he/she uses the client's contact details. Also, when preparing claims on behalf of the client, legal practitioners use their personal data to individualise the claim, etc.

4.4. Dissemination or otherwise making available

In today's high-tech society, activities such as online sharing and publication of information are performed almost routinely. However, they most often qualify as processing of personal data and therefore fall under the scope of data protection regulations. With this respect, the CJEU has found in its judgement on case C-101/01, *Bodil Lindqvist v Åklagarkammaren i Jönköping*, that the operation of loading personal data on an internet page must be considered to be processing. Pursuant to the opinion of Advocate General (AG) Tizzano under this case *"loading [...] information on a home page [...] gives rise to*

[40] CJEU, Judgement on case C-73/07, *Tietosuojavaltuutettu v Satakunnan Markkinapörssi Oy, Satamedia Oy*, 16 December 2008, para. 37

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

a "processing" of personal data since, in that respect too, the Directive contains a particularly wide definition covering "any operation or set of operations which is performed upon personal data, whether or not by automatic means such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction" (Article 2(b))." The Court followed the opinion of AG Tizzano in this respect and held that the examples given by the provisions of Art. 2 (b) of the Directive 95/46 (respectively Art. 4, No. 2 GDPR) are clear enough so as to hold that the operation of loading personal data on an internet page must be considered to be processing.[41]

This conclusion was upheld in CJEU judgement on case C-230/14, *Weltimmo s. r. o. v Nemzeti Adatvédelmi és Információszabadság Hatóság* of 1 October 2015. The Court found that the running of one or several property dealing websites concerning properties and the publication, on these websites, of personal data relating to the owners of those properties and, in some circumstances, of the use of those data for the purpose of the invoicing of the adds consists of an operation of loading personal data on an Internet page and should, without a doubt, be considered 'processing' within the meaning of Article 2(b) of Directive 95/46/EC.

Example: a law firm has its own webpage where all attorneys practicing at the firm have their biography and photos uploaded.

4.5. Other types of processing activities

Besides Collection, Recording and Storage, Use, Dissemination or otherwise making available, there are other types of activities that are regarded as personal data processing. The following list of activities showcasing such other types of action that should be considered data processing is not exhaustive, but sheds further light to legal practitioners in view both their practice and daily activities as data controllers/ processors:

- Organisation and structuring - organisation and structuring of information is a form of

[41] *Lindqvist,* Para. 25

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

processing of personal data which may be seen, for instance, in the practice of storing patient medical files in medical practices or hospitals, creating a list of employees' contracts in an enterprise, etc. organising clients' cases by a chronological order;

- Adaptation or alteration - any adaptation or alteration of data, no matter how insignificant, would amount to processing and be treated as such.

An example for such processing would be application of encryption techniques which adapt the format of the data.

- Retrieval or consultation - such processing may involve, for instance, the fact for a potential employer to check, during the recruitment process, the profiles of the candidates on various social networks and includes information from these networks (and any other information available on the internet) in the screening process;
- Disclosure by transmission - the CJEU discussed the disclosure and the dissemination of data in its reasoning in the framework of the *Bavarian Lager* case. The proceedings involved a discussion of whether the minutes of a meeting containing names of the participants may be revealed upon request based on the right to public access to European Parliament, Council and Commission documents. Amongst other findings, the General Court held that "*communication of data, by transmission, dissemination or otherwise making available, falls within the definition of "processing"*.[42] Although, on the main proceedings the Court of Justice set aside the judgment of the General Court, it upheld its finding that, by virtue of the very definition of the concept of "processing of personal data", the communication of personal data (namely the names of attendees to a meeting) falls within the definition of 'processing';[43]
- Alignment or combination;

An example of such processing is the matching of data concerning health that has been collected over a certain period of time.

[42] General Court, Judgement on Case T-194/04, *The Bavarian Lager Co. Ltd. v Commission of the European Communities*, of 8 November 2007, para. 105
[43] ECJ, Judgement on Case C-28/08 P, *European Commission v the Bavarian Lager Co. Ltd*, of 29 June 2010, para. 69

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

- Restriction - as a type of processing restriction comes to replace "blocking" as outlined in Directive 95/46/EC. Restriction activities will include any type of activity that makes the access to some information unavailable. The restriction as a type of processing should be differentiated from the definition of "restriction of processing"[44], which constitutes itself data processing. The definition of the "restriction of processing" comes to clarify the provisions in relation to the right to restriction. However, the scope of restriction as a type of processing cannot be limited only to cases, where the right to restriction is exercised.
- Erasure or destruction (digital or physical) – although it might not seem like a processing activity, even the erasure of personal data is a processing activity. To this end, the physical shredding of documents encompassing personal data is in fact processing.

An example of such type of processing of personal data in a digital environment will be the terminal deletion of file containing personal data records in a cloud-based storage system.

Key concepts:

Activities of data processing: any operation or set of operations performed upon personal data or sets of personal data regardless of the means (automated or not) used; examples for such operations are 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.

Collection: Any collection of information from the individual to whom the personal data relates or from a third party is considered "processing".

Recording and Storage: any variation of these operations is also always considered data processing.

Use: any use that is not explicitly excluded is considered processing (such is personal or household activity with no connection to a professional or commercial activity).

[44] In accordance to Article 4, No 3 'restriction of processing' means the marking of stored personal data with the aim of limiting their processing in the future;

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

Dissemination: it most often qualifies as processing of personal data.

Most important notions for legal practitioners: Most activities should be assessed on an ad hoc basis to determine if they constitute data processing or not.

Chapter 5: Who is data controller and who is data processor?

5.1. Notion

The importance of the distinction between the two terms lays in the different scope of responsibility data controllers and data processors bear. Legal practitioners should consider the differences both in relation to their own practice and in relation to their clients. The correct determination of the position of a certain entity is crucial for establishing its obligations under the GDPR.

5.1.1. Data Controllers

The definition of data controller (Art. 4, Para. 7) contains two criteria: 1) to be a natural or legal person, public authority, agency or other body, and 2) to determine alone or jointly with others the purposes and means of the processing of personal data. The emphasis is on who has the discretion in determining purposes and on the latitude of making decisions[45].

According to the Article 29 Working party's opinion, "means" does not only refer to the technical ways of processing personal data, but also as to "how" processing occurs, which includes which data shall be processed, which third parties shall have access to this data, when the data will be deleted and other matters[46]. Some technical aspects of the processing could be delegated to a processor, if they are not essential for the control of the processing[47] (essential aspects could be the ones related to security,

[45] Article 29 Data Protection Working Party, Opinion 1/2010 on the concepts of "controller" and "processor", adopted on 16 February 2010, WP169, p. 15
[46] Ibid., p. 16
[47] Ibid., p. 14

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

but this is not necessary). The means should represent a reasonable way of achieving the purpose and the data controller should be fully informed about them[48].

Regarding corporate groups, it is important to note that each company within a group may be a data controller in respect of the personal data which it has obtained, which it controls and for which it is legally responsible[49].

The personnel in a controller (a company or other legal entity) are acting under the authority of the controller and are bound by the provisions of Art. 29 of the GDPR if they have access to data. They must process that data following the instructions from the controller or if required to do so by Union or Member State law. If a natural person acting within a legal person (i.e. an employee) uses data for his or her own purposes outside the scope and the possible control of the legal person's activities, it should be considered a controller and bear the respective responsibility. The original controller could nevertheless also bear some responsibility regarding the lack of adequate security measures[50].

5.1.2. Joint controllers

The GDPR further regulates the cases where the purpose and means of the processing are determined by various entities together. In such a case those entities, called joint controllers, share data protection obligations under the GDPR and therefore have to determine in a transparent manner their respective responsibilities. Joint controllers must enter into an arrangement, which reflects their roles and relationships regarding the data subjects, especially when it comes to the subjects' rights to information. The essence of the arrangement must be available to the data subjects and the controllers may designate one common contact point for them. Regardless of the terms of the arrangement, subjects can still exercise their rights against each of the controllers. It is important to note that the GDPR does not

[48] Ibid.
[49] Voigt P. and von dem Bussche A., *"The EU General Data Protection Regulation (GDPR). A Practical Guide"*, Springer International Publishing AG 2017, p. 18
[50] Article 29 Data Protection Working Party, Opinion 1/2010 on the concepts of "controller" and "processor", adopted on 16 February 2010, WP169, p. 18

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

require a contract, the arrangement can be in any form permitted by national law, for example joint privacy statements, terms and conditions, or policies[51].

It is important for entities to determine if they are separate controllers, a controller and a processor or joint controllers, because of the specific rules for joint controllers stated above. No explicit administrative penalties are provisioned in the GDPR for violating these obligations, but incompliance with them could be considered a general incompliance with the principles of the Regulation. To determine whether the entities act as joint controllers, it should first be determined whether the relationship between them requires processing the same personal data, or just sharing the same pool of personal data for different and distinct purposes. It should be taken into consideration if and to what extent relevant decisions are taken together by the parties and how the processes themselves are intertwined[52].

An example of joint controllership given by the Article 29 Working party is using a recruitment (head-hunters) company to find new staff. The Working Party considers that a recruitment company and a hiring company would act as joint controllers at least regarding those sets of operations related to the recruitment of the particular company[53]. As opposed to this example, travel agencies, hotels and airlines are considered separate controllers regarding data of clients purchasing travel packages, because each of them uses the data for own purposes using different means. However, if for example the travel agency, the hotel chain and the airline decide to set up an internet platform, they will process data after agreeing on certain aspects (like which data will be stored, how reservations will be allocated and confirmed and who can have access to the information stored). Therefore, they will take decisions regarding the purposes and means together and will become joint controllers[54].

Understanding the particularities of joint controllership is of high importance to the target group of the current report as legal practitioners need to be aware how to consult a client regardless if the client

[51] Foitzik, Piotr, How to comply with provisions on joint controllers under the GDPR, 26 September 2017, available at: https://iapp.org/news/a/how-to-comply-with-provisions-on-joint-controllers-under-the-gdpr/
[52] Ibid
[53] Article 29 Data Protection Working Party, Opinion 1/2010 on the concepts of "controller" and "processor", adopted on 16 February 2010, WP169, p. 19
[54] Ibid, p. 20

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

is a controller/ processor which requires consultancy on how to determine contractual relationships or a data subject which claims his/ her rights under GDPR have been violated.

5.1.3 Data processors

According to the definition of Art. 4, No. 8, a data processor is *a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller*. The main characteristics of the processor are: 1) a separate entity from the controller and 2) processor of data on behalf of the controller. The existence of a processor depends on a decision taken by the controller, who can either process data within its organisation (e.g., through its own employees) or delegate all or part of the processing activities to an external organisation, rendering the latter a "processor"[55]. It is possible that several processors are instructed to act on behalf of the controller at the same time. Any processor exceeding his or her the limits determined by the controller and acquiring a relevant role in determining the purposes or essential means of data processing turns into a (joint) controller (Art. 26, para. 10 GDPR).

5.2. Determination based on the definitions in Art. 4, No. 7 and 8

When determining if an entity is a controller or a processor, a few criteria based on its influence on the purposes and/or means of processing may be applied:[56]

- Freedom from instructions by the contracting entity that delegated the data processing;
- Merging of the data received upon delegation with own databases;
- Use of the data for own purposes that may have not been agreed upon with the contracting entity;
- Processed data having been collected by way of a legal relationship between the processing entity and the data subjects;
- Responsibility of the processing entity for the lawfulness and accuracy of the data processing.

[55] Ibid, p. 27
[56] Voigt, P., von dem Bussche, A., The EU General Data Protection Regulation (GDPR), A practical guide, Springer, 2017, p. 19

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

Typical examples of data processors are entities such as cloud services, IT support, data centres.

They have access to the data but cannot process it in any way outside the narrow field of their services. An example of controller and processor is a telecom company outsourcing its customer support to an external call centre. The call centre can process data only for two purposes, determined by the telecom company: to take on calls and communicate the problems the clients are experiencing to the company and to call customers periodically to offer them services. In this situation the call centre is a processor. If the manager of the call centre decides to call customers to offer them services of other clients of theirs, without having authorisation by the telecom company, the call centre has to be considered a data controller, because it is acting outside the scope of the instructions it received from the controller.

5.3. Critical cases regarding the target groups

Taking into account INFORM's target groups, it should be noted that law firms are considered data controllers[57], because they process the data of their clients as well as the data of their partners and staff. A law firm handling a litigation case on behalf of a client processes the client's personal data. Under GDPR the firm must make the client aware of why they need their personal data and how they are going to use it in relation to the handling of the case. If the firm appoints an expert witness, the expert witness should be classed as a 'data processor' as they process the client's personal data, but they are acting under instruction from the law firm.

For legal practitioners in would be rare to act as joint controllers as their usual activities exclude such possibility. Such a scenario is plausible when separate legal practitioners work together on a case/ project as the parties in such a case determine jointly the purposes and the means for data processing.

[57] ICO Guide, Data controllers and data processors: what the difference is and what the governance implications are, p. 9-10, available at: https://ico.org.uk/media/for-organisations/documents/1546/data-controllers-and-data-processors-dp-guidance.pdf; O'Rorke, Owen, Under control?, 4 July 2017, available at: http://communities.lawsociety.org.uk/law-management/magazine/july-2017/under-control/5062090.fullarticle

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

Key concepts:

Data Controller: natural or legal person, public authority, agency or other body which determines alone or jointly with others the purposes and means of the processing of personal data.

Data Processor: natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller and is a separate entity from the controller.

Most important notions for legal practitioners: it should be determined if the entity is a controller or a processor regarding each particular processing activities. Legal practitioners should keep in mind that almost all entities are controllers at least regarding the data of their own employees. Law firms are considered controllers regarding their clients' data.

Chapter 6: Lawfulness of processing, Art. 6 ("Rights" of the data controller)

The subject of this section constitutes another building block for the right application of the GDPR. Legal practitioners should carefully examine the conditions for lawful processing regardless of whether they defend data controllers or data subject's rights. The right understanding of the relationship between the six different legal bases for lawful processing of personal data regulated by GDPR is equally important. In this regard, it should be noted that the particular legal basis for each processing must be established prior to the start of the processing activities[58]. Furthermore, the controller cannot switch between the different legal bases. Once the legal basis for processing is determined, it cannot be changed amidst the processing activities to better suit the overall operation of the data controller. Below, each of the legal bases is examined in a manner that ensures proper understanding of the concept of lawful processing under the GDPR.

[58] Article 29 Working party, Guidelines on Consent under Regulation 2016/679, WP259, p.22.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

6.1. Consent of the data subject

Consent is a cornerstone notion in the system of personal data protection as it reflects the importance of the respect of the free will expressed by the data subject. To this end, the European legislator has - paid specific attention towards the regulation of this particular legal basis for personal data processing. The legal definition of consent is set in Article 4, No. 11 of the GPDR, where it is outlined as *"any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her."* In addition, Article 7 prescribes the conditions for obtaining valid consent. These two articles should be construed in the light of Recitals 32, 33, 42, 43.

The issue of the "consent" has been a subject of analysis by Article 29 Working party numerous times, and recently the Working party has issued dedicated Guidelines on Consent under Regulation 2016/679[59]. In this document, the Working party underlines once again that consent offers control to the data subject as a guarantee for his/ her free will in terms of the execution of any data processing activities. The Guidelines further emphasise that the obtained consent does not override the key principles for data processing enshrined in Art. 5 of GDPR such as data minimisation, fairness and proportionality of the data processing activities, etc.[60] Another critical characteristic of consent as a legal basis for personal data processing is the right of the data subject to withdraw the consent at any time without the obligation to state a reasoning behind this decision. The establishment of the right of withdrawal, outlined in Art. 7, para. 3, comes to show that indeed the data subject retains control of the situation and again serves to demonstrate that the data subject had a choice and a free will before consenting to any type of data processing.

The main elements of the consent that derive from the definition enshrined by Art. 4, No. 11 GDPR. These elements should be all present (the requirements are cumulative) when determining whether the consent does constitute a valid legal basis for processing:

- freely given;

[59] Ibid
[60] Ibid., p. 4.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

- specific;
- informed; and
- unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

In order to consider the consent freely given, one should examine whether the data subject has had on his/ her disposal a real choice. Data subject will have a real choice when she or he does not feel compelled to give his/her consent and when there is no negative consequence for not wanting to consent. In Recital 43 the EU lawmaker -included a presumption for the absence of consent in cases "*where performance of a contract, including the provision of a service, is dependent on the consent despite such consent not being necessary for such performance*".

For example, in case where a registration on a website, providing e-learning courses, includes a mandatory requirement to the user to agree to the processing of personal data for marketing purposes, the consent for the latter shall not be valid. In this case the user is compelled to give his/her consent for the processing of his/her personal data for marketing purposes, despite the fact that this processing is not necessary for the provision of the educational service. Another good example of invalid consent takes place in cases of non-negotiable parts of the terms and conditions of a contract.

Another prerequisite for valid consent is that it is specific, meaning that consent is obtained for a specific reason. This condition further affirms that consent is a legal basis ensuring that the power balance is maintained, and it is the data subject that ultimately controls how their data is processed. In order for one to evaluate whether the consent is indeed specific, firstly the purposes for the processing should be clearly defined. If the processing will be executed for more than one particular purpose, then the data subject must be provided with the option to freely choose to which of the available purposes of data processing he/ she consents to. To effectively observe this requirement the processor must provide the data subject with opt-in regime and enable him/ her to express their free will in view of the different types of data processing they consent to. Finally, the controller should outline the specific

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

types of data that will be processed. To this end, when choosing, data subjects must be provided with information what type of data is processes for what type of purpose.

The legislator - laid down the requirement that the valid consent is the informed consent. Essentially, what is necessary for the consent to be informed is to provide knowledge to the data subject concerned what he/ she is agreeing to, how to exercise the right to withdrawal, the identity of the controller and their contact details, if any automated decisions will be made in view of the data subjects, if data transfers to third countries might occur. In addition, the information outlined above must be provided in a clear, plain and accessible language, refraining from the usage of specialised terminology or confusing phrasing.

The last cumulative requirement for valid consent is that the data subject expresses his/ her consent in unambiguous manner reflecting an active declaration. In other words, it is required that the data subject expresses consent through clear affirmative action. The latter means that the natural person must take deliberate actions to consent such as clicking on a box, signing a written form, verbally expressing consent[61] with the particular data processing activity. To comply with this requirement, the request for consent should not be a blanket clause incorporated in general terms and conditions to a contract. The blanket acceptance of terms and conditions does not constitute clear affirmative action and cannot demonstrate that the data subject has made a particular decision pursuing their free will.

In the daily activities of legal practitioners, the consent will be the applicable legal basis for adding the contact details of a client of the law firm to a newsletter mailing list.

6.1.1. Explicit consent

The European legislator - recognises that processing of personal data for a number of specific cases requires the obtainment of explicit consent. The European legislator has listed exhaustively these cases. To this end, explicit consent is required for the processing of special categories of data provided for in Art. 9 of the GDPR, for personal data transfers to third countries or international organisations

[61] Please note that if the consent is expressed orally, it must be recorded, so the data controller/ processor is able to demonstrate the collection of a valid consent.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

where adequate safeguards are missing (Art. 49, para. 1, lit. a, GDPR), and in cases where the data subject concerned could be affected by automated decision-making, including profiling (Art. 22 GDPR).

As the prerequisites for valid consent already require that the consent is free, specific, informed and unambiguous, one might ask if there are any additional prerequisites which make consent explicit. What constitutes a consent as explicit is the manner it is manifested – the data subject ought to make an expressive statement consenting with the data processing. In the 'paper' environment, such an action would be the handwritten signature of the data subject concerned. In an online environment, the explicit consent might be expressed using a qualified electronic signature, sending a dedicated email (i.e. an email with solely "I agree" in the body), utilising a two-step verification process[62].

From the viewpoint of legal practitioners, it is important to note that the data controller must be able to demonstrate the obtainment of such explicit consent. The data controller must be able to demonstrate at every single moment that valid consent has been expressed to every single type of data processing, for every single purpose outlined by the data subject in his/ her consent. To this end, it is advisable that the data controller maintains such expressions of consent that could be easily demonstrated as written forms and qualified electronic signatures. For innovative business models, another piece of technology that could be used for this task is the blockchain.

While performing the usual activities of legal practitioners, consent will rarely be used, as they process the data of their clients on the basis of a contract or in order to take steps at the request of the data subject prior to entering into a contract (when the client is a natural person, otherwise it will be the legitimate interest of the legal person). Regarding other data subjects, the legal practitioners will mostly act on the basis of their own legitimate interest or the legitimate interest of a third party (for example when processing data of the opposite party in proceedings the basis will be the legitimate interest of the client). It is not advisable to legal practitioners to make their clients sign declarations of consent for their personal data to be processed, since consent should

[62] Article 29 Working party, Guidelines on Consent under Regulation 2016/679, WP259, p. 19.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

be used only when there are no other legal grounds for processing and in the case of legal practitioners such grounds are present[63].

6.1.2. The right to withdraw consent

Although the consent for personal data processing is not bound by any time limit, the data subject has on his/ her disposal the right to withdraw consent at any time. The establishment of the data subject right to withdraw consent once again underlines that the control is indeed within the individual, and he/ she can freely act upon their will. What Art. 7, para. 3 of the GDPR stipulates is that the exercise of the right to withdraw consent must be as easy as the initial expression of consent. The provision regulates the manner, and not the actions – hence there is no legal obligation that the consent is withdrawn through the same action that has been used by the controller to obtain the data subject's consent.

A data subject might express consent by submission of a digital form, using qualified electronic signature and sending an email to the controller to exercise his/ her right to withdraw consent.

At the same time, the data controller should not place any specific requirements which may burden a natural person in their desire to withdraw consent. Therefore, the data controller must accept every manifestation by a natural person reflecting the will of the individual to withdraw consent.

What is important to note here in view of GDPR application and interpretation by legal practitioners is that in the moment the controller receives the withdrawal, they must cease any processing of the personal data concerned based on consent, and either delete this data or render it anonymised.

[63] For instance, one cannot ask for the consent of the data subject for processing his/her data for the purposes of executing a contractual obligation, as there is the hypothetical possibility that the data subject withdraws his/her consent. That means that – without having the contract terminated, parties will not be able to execute their obligations – for instance paying to the party without having its bank account. Another example can be given for the processing of personal data of the data subject, who constitutes an opposite party to a dispute. It cannot be expected that legal practitioners must request the consent of the opposite party, when processing their data, as this will most definitely prevent them from defending the rights of their clients – the opposite party may not give its consent, or may withdraw it at any time.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

6.2. Performance of a contract (Art. 6, para. 1, lit. b)

Another legal basis that provides for in lawful processing of personal data is the performance of a contract. Such processing is lawful when it is necessary for the performance of a contract to which the data subject is party or for taking steps at the request of the data subject before entering into a contract. The notion 'performance of a contract' has to be construed in a wide manner and concerning any phase of the contract[64]. Processing is deemed necessary if the contract could not be fulfilled without the processing taking place. Necessary does not mean that the processing must be essential for the purposes of performing a contract or taking relevant pre-contractual steps. What this notion means is that such processing of personal data must be a targeted and proportionate way of achieving the purpose of performing of a contract[65]. In other words, there should not be any less intrusive ways besides the processing of the personal data in question to meet the contractual obligations or take the steps requested. This has to be determined on a case-by-case basis[66].

For example, when a data subject makes an online purchase, a controller processes their address in order to deliver the goods. This is necessary to perform the contract. However, the profiling of an individual's interests and preferences based on items purchased is not necessary for the performance of the contract and the controller cannot rely on Article 6, para. 1, lit. b as the lawful basis for this processing[67].

If a data controller is processing personal data on the basis of a contract, the individual's right to object and right not to be subject to a decision based solely on automated processing will not apply (Art. 21, para. 1 and Art. 22 para. 2, lit. a). However, the data subject will have a right to data portability Art. 20 para. 1, lit. a. If the processing is lawful on the basis of a contract, no separate consent is

[64] Voigt, P., von dem Bussche, A., The EU General Data Protection Regulation (GDPR), A practical guide, p. 102, Springer, 2017
[65] ICO guide, Lawful basis for processing, available at: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/contract/
[66] Voigt, P., von dem Bussche, A., The EU General Data Protection Regulation (GDPR), A practical guide, p. 102, Springer, 2017
[67] ICO guide, Lawful basis for processing, available at: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/contract/

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

needed. Furthermore – the obtainment of such is redundant and cannot be used as 'plan b'. If processing of special categories of personal data is necessary for the contract, the data controller must identify a separate condition for processing this data[68]. Data processing activities by the controller for the purposes of a contract between the data subject and a third party could be covered by this permission, as Art. 6, para. 1, lit. b requires the data subject, not the data controller to be party to the contract.

When processing data for performing their activities, it is advisable for legal practitioners to use this basis for processing the data of their clients (see p. 6.1), when they are natural persons When their clients are legal persons, the applicable legal basis for processing personal data of data subjects by legal practitioners will be in most of the cases - the legitimate interest of the legal person.

6.3. Compliance with a legal obligation (Art. 6, para. 1, lit. c)

This legal basis for processing is applicable when the data controller must process data to comply with the law. The processing must be necessary, or in other words, if the controller can reasonably comply without processing the personal data, this basis does not apply. The obligation does not necessarily have to derive from legislative act adopted by the national legislature (Recital 41) but can also derive from secondary legislation. The legislation must be clear and precise and its application to be foreseeable to its subjects. This does not mean that there must be a legal obligation specifically requiring the processing activity, but that the overall purpose must be to comply with a legal obligation imposed on the controller[69]. Such activity may be compliance with a court order, with binding instructions of a state body or with regulatory requirements.

Example: passing data to a regulatory body to conduct a social welfare assessment

[68] Ibid.
[69] Ibid.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

Again, the processing performed should be a reasonable and proportionate way of achieving compliance[70]. It should also be noted that Member States may introduce additional specific requirements for such types of processing (Art. 6, para. 2). Under this legal basis for processing, the data subjects are not entitled to the right to erasure, right to data portability, or right to object.

In the light of the target group of this particular review report, it should be noted that lawyers enlisted in the national bodies responsible for the provision of legal aid free of charge, will process data on this particular legal basis once assigned with a case. Similar is the case of personal data processing by bailiffs and notaries. Furthermore, the correct construe of this legal basis calls for careful examination of each case a legal practitioner is contracted to defend data controllers'/ data subject's right as national legislation could indeed provide a wide array of options to provide for personal data processing pursuing compliance with legal obligation.

6.4. Protection of the vital interests of the data subject (Art. 6, para. 1, lit. d)

As situations where the vital interest of an individual is endangered occur, GDPR also regulates the lawful processing of personal data in such instances as well. Under the GDPR vital interests of both data subjects and other natural persons could be legal basis for processing. According to Recital 46 processing of personal data based on the vital interest of another natural person should take place only where the processing cannot be manifestly based on another legal basis. It's clear from Recital 46 that vital interests are intended to cover only interests that are essential for someone's life. This legal basis is relevant to emergency medical care, when the individual is incapable of giving consent to the processing[71] or in cases of a natural or man-made disaster. However, health data is one of the special categories of data, which means a condition for processing of special categories of personal data under Article 9 must be present. There is a specific condition under Article 9, para. 2, lit. c for processing special categories of data where necessary to protect someone's vital interests.

[70] Ibid.
[71] According to ICO Guide, Lawful basis for processing, available at: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/contract/

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

With respect to legal practitioners this legal basis is important when defending the rights of their clients.

6.5. Performance of a task in the public interest (Art. 6, para. 1, lit. e)

This legal basis could be used under one of two conditions: if the processing is necessary for the performance of a task carried out in the public interest or if the controller exercises official authority vested in him or her. If a controller can prove that he or she is exercising official authority, there is no need to prove there is also public interest present. However, the processing should be 'necessary' for the purpose in all cases (Art. 6, para. 3). The latter is most relevant to public authorities, but it can apply to any organisation that fulfils the conditions. The basis for the processing shall be laid down by either EU law or national law to which the controller is subject and shall comply with the general requirements of Recital 41 -*to be clear and precise and its application to be foreseeable to persons subject to it*-. No specific legal authority is needed for the particular processing activity, as long as the overall purpose is to perform a public interest task or exercise official authority[72]. Data subjects' rights to erasure and data portability could not be exercised when data processing occurs under this legal basis. They, however, are entitled to the right to object (Art. 21, para. 1). If processing of special categories of personal data is in place, the controller needs to identify an additional condition for the processing of this type of data.

- For legal practitioners in particular, it is quite important to always determine if certain processing activities are carried out in public interest and to always identify the legal act stipulating controller's prerogatives in this direction.
- This basis will not generally be used by legal practitioners, acting as attorneys. This legal basis, considering the specifics of the national legislation, will be applicable to bailiffs and public notaries.

[72] Ibid

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

6.6. Purposes of the legitimate interest (Art. 6, para. 1, lit. f)

The sixth legal basis provided for in GDPR regulates processing when necessary for the purposes of the legitimate interest pursuit by the controller or by a third party. This legal basis cannot be applied when such interests are overridden by the interests or fundamental rights and freedoms of the data subject, especially in cases where the data subject is a child. Therefore, an assessment of the interests should be made, and the processing will be lawful only when the legitimate interests of the controller or third party prevail over the fundamental rights of data subjects. The legitimate interests of children must be taken into specific consideration. It is also important that processing on this legal basis should be necessary, otherwise it is unlawful.

When the basis for processing is the legitimate interest of a controller, it is the controller who carries the burden of proof in view of their legitimate interests. The legitimacy of the interests is considered in relation to the specific processing situation, and they might be of a legal, economical, idealistic or other nature[73]. The GDPR gives examples for legitimate interests: where the processing is executed in an intra-group for internal administrative purposes, when disclosing information network information security incidents to the competent authorities. (Recitals 47, 48, 49 and 50). It is important to assess if the data subject can reasonably expect at the time and in the context of the collection of the personal data that processing for that purpose may take place. According to Recital 47, if data subjects do not reasonably expect further processing, their interests and fundamental rights could override the interest of the data controller. It is explicitly stated that the processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest (Recital 47, 70). However, legitimate interest as legal basis for personal data processing does not apply to the processing by public authorities in the performance of their tasks, as they are conducting processing activities on other legal basis, outlined above.

An example for legitimate interest of a controller that must be juxtaposed to the interests and fundamental rights of data subject could be using cameras on the premises of an employer. If the

[73] Voigt P. and von dem Bussche A., *"The EU General Data Protection Regulation (GDPR). A Practical Guide"*, Springer International Publishing AG 2017, p. 103

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

cameras are in working areas, this data processing may be rendered necessary and proportionate. However, if they are placed in rooms for lunch or rest, there is high probability that this processing may infringe the data subjects' (in this case the employees') rights.

When processing is performed on this legal basis, the data subjects are entitled to the right to object to the processing (Art. 21, para. 1).

- As stated above, this basis will be used by legal practitioners in all the cases where they are processing data of persons who are not a party to a contract (clients). It will be the grounds for processing all kinds of information connected with, for example, other participants in legal proceedings.

6.7. Restrictions (of the rights of the data subjects), Art. 23

Under certain circumstances the rights of data subjects and the corresponding obligations of data controllers could be restricted. First, such a restriction should be imposed with a legislative measure. Second, it should respect the essence of the fundamental rights and freedoms. Third, it should be a necessary and proportionate measure in a democratic society and fourth - its purpose should be to safeguard certain interests, which are enumerated in Art. 23, para. 1, lit. a-j and which are *numerus clausus* (national security, public security, the protection of judicial independence and others). Such legislative measure should contain specific provisions - the purposes of the processing or categories of processing, the categories of personal data, the scope of the restrictions introduced, the safeguards to prevent abuse or unlawful access or transfer and others (Art. 23, para. 2). If such national measures lessen the obligations of data controllers, they should be able to demonstrate how the national provision in question applies to them[74]. The data controllers should inform data subjects that they are relying on such a national legislative restriction, unless doing so would be prejudicial to the purpose of the restriction (Article 23, para. 2, lit. h).

- In this regard, legal practitioners should follow closely the national legislation which may permit such restriction of rights. It is highly probable for some legal professions to not be affected by all

[74] Article 29 Data Protection Working Party, Guidelines on transparency under Regulation 2016/679, WP260, p. 30

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

the obligations of data controllers to data subjects, given the specifics of their activities and the obligations connected with the professional secrecy.

Key concepts:

Lawful basis for processing: in order to be lawful, every processing should be based on one of the grounds in Art. 6, para. 1, lit. a-f.

Most important notions for legal practitioners: for legal practitioners the most relevant bases for personal data processing are the performance of a contract or the taking of steps prior to entering into a contract and compliance with legal obligation (Art 6, para. 1, lit. b and c). Keep in mind that consent is a subsidiary basis when no other grounds for processing could be found and it will rarely be applicable in the work of legal practitioners (the exception could be for example a form on a site when the filing of the form does not constitute steps towards entering into contract). Legal practitioners should also pay attention to the national legislation and the possible lessening of the obligations of controllers permitted under Art. 23.

Chapter 7: Obligations of the data controller

The GDPR places data controllers at the centre of data protection obligations and further extends their responsibility and liability. Art. 5, para. 2 GDPR establishes the general rule of accountability which requires data controllers to ensure compliance with the Regulation obligations as well as to be able to prove for such compliance. Violations of the accountability principle may lead to fines of up to EUR 20 000 000 or up to 4% of the total worldwide annual turnover of the organisation (Art. 83, para. 5 GDPR). The increased pecuniary sanctions call for a strengthened and effective data protection strategy of controllers, starting with their organisational obligations.

7.1. Organisational obligations

Organisational obligations of data controllers are laid down in Articles 24 to 31 GDPR. For the most part, these provisions confirm the pre-existing rules established by the Data Protection Directive.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

However, the GDPR establishes some new fundamental principles and introduces a series of new organisational requirements which will call for some significant efforts of controllers in order to ensure compliance with GDPR.

7.1.1. Responsibility of the controller (Art. 24; Recitals 74-79)

Pursuant to Art. 24 GDPR, and in line with the accountability principle, controllers are required to implement technical and organisational measures in order to ensure and to be able to demonstrate compliance with data protection regulations. The same obligation is introduced with Article 19, paras. 1 and 2 of Directive 2016/680.

Identification of the assets

The accountability principle embedded in Art. 24 GDPR, is built upon the general risk-based approach adopted by the Regulation. The measures which the controller is required to adopt pursuant to Art. 24 GDPR should be identified based on an objective case-by-case assessment and will thus depend on circumstances such as the nature, scope, context and purposes of processing as well as the various risks for the rights and freedoms of individuals.

Controllers are thus required:

- To implement appropriate technical and organisational measures to ensure and be able to demonstrate compliance with data protection obligations, *including the effectiveness of the implemented measures* (Recital 74 GDPR).
- To regularly review and, when necessary, update implemented measures.

Technical and organisational measures are increasingly referred to as "privacy management programs", e.g. internal compliance systems[75], and become a fundamental element of data protection legislation. They are planned to account for, where relevant, the privacy-by-design and by-default principles and are intended to reflect processing risks and effectively mitigate their effects.

[75] Voigt P. and von dem Bussche A., "The EU General Data Protection Regulation (GDPR). A Practical Guide", Springer International Publishing AG 2017, p. 33

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

Installation of appropriate protective measures - what kind of measures are expected? Extensive interpretation. Rules of conduct. Accountability/demonstrability (Art. 30)

Art. 24 GDPR does not provide extensive details on how measures should be identified and implemented. Nonetheless, its para. 2 establishes that, where relevant, measures should include the implementation by the controller of appropriate data protection policies. According to some authors, the implementation alone of data protection policies will not be sufficient to satisfy compliance with the Regulation obligations.[76] In order to be able to prove that compliance is effectively achieved, controllers shall introduce and objectively document their efforts deployed for the purposes of ensuring respect to data protection obligations.

Pursuant to Recital 77 GDPR controllers may use and benefit from guidelines provided by the European Data Protection Board (the Board) established by the Regulation, or from indications provided by a data protection officer. It is indicated that the Board may issue guidelines on processing operations that are considered to be unlikely to result in a high risk to the rights and freedoms of natural persons and indicate what measures may be sufficient in such cases to address such risk.

In addition, pursuant to Art. 24, para. 3 GDPR adherence to approved codes of conduct or approved certification mechanisms may be used by the controller as an indicator for compliant processing. Certification mechanisms may be used by legal practitioners. However, it should be borne in mind that certifications as such do not reduce the responsibility of the controller for compliance with the Regulation. Data controllers, legal practitioners included, need to deploy real and effective efforts to safeguard and respect data protection principles. It is probable that many national organisations, such as bar councils, may develop codes of conduct for different branches of the legal profession (for example for law firms and lawyers).

[76] Baker & McKenzie LLP, *Accountability Obligations under the GDPR*, available at http://globalitc.bakermckenzie.com/files/Uploads/Documents/Global%20ITC/13%20Game%20Changers/BM-Accountability%20Obligations%20under%20the%20GDPR.pdf, p. 2

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

Data controllers should develop and observe data protection policies regulating for instances – retention policy, policy for document destruction, policy for access control – including biometric identification, policy for account and passwords management, etc.

Risk level and likelihood (Recital 75)

The likelihood and severity of the risk to the rights and freedoms of the data subject is determined by reference to the nature, scope, context and purposes of the processing (Recital 76 GDPR).

Risk should be evaluated on the basis of an objective assessment and on a case-by-case basis, in order to establish whether data processing operations involve a risk or a high risk (Recital 76 GDPR). This evaluation should take into account potential threats to the rights and freedoms of individuals leading to physical, material or non-material damage. The non-exhaustive list of examples of threats and potentially problematic processing, provided by Recital 75 GDPR, includes:

- Processing resulting in or able to give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorised reversal of pseudonymisation, or any significant economic or social disadvantage;
- Processing leading to deprivation of data subjects of their rights and freedoms or prevention from exercising control over their personal data;
- Processing of special categories of data or of data relating to criminal offences;
- Processing for the purpose of profiling;
- Processing of personal data of vulnerable individuals, namely of children;
- Processing involving a large amount of personal data and affecting a large number of data subjects.

In case controllers process personal data in conditions close to the hypothesis listed above or otherwise qualified as risky or highly risky, they should cautiously consider their obligations under Art. 24 and

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

following GDPR and apply respective measures and safeguards. Considering the data that legal practitioners process of their clients, it is highly probable that this processing poses a high risk to the data subjects' rights in accordance with the examples given in Recital 75, especially in its hypothesis concerning personal data protected by professional secrecy.

Reasonableness of measures, balancing of interests (Art. 24 para. 2 GDPR, Art. 52, para. 1 the Charter)

- Pursuant to Art. 24 GDPR when deciding upon technical and organisational measures to apply in view of GDPR compliance, an evaluation need to be made in terms of proportionality with processing activities. Implemented measures need to be reasonable compared to those processing activities. This balancing of interests is in line with the general EU principle of proportionality, embedded in various legal acts, including the Charter of Fundamental Rights of the European Union (the Charter), Art. 52, para. 1 of which reads: *"Any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognized by the Union or the need to protect the rights and freedoms of others."*
- In the case of legal practitioners, they may have special obligations for securing their clients' data under special laws and requirements connected with the professional secrecy. The measures taken in regard to these obligations may be enough to comply with the requirements under the GDPR, but still it is advisable that an assessment is made.

7.1.2 Record of processing activities, Art. 30 (rec. 82, 89)

Pursuant to Art. 30 GDPR data controllers, as well as, where applicable, their representatives, are required to maintain a record of processing activities under their responsibility. The record should be maintained in writing, including in electronic form (Art. 30, para. 3 GDPR).

The records of data controllers should encompass the following information:

- Name and contact details of the controller and, where applicable, the joint controller, the controller's representative, and the data protection officer;
- Purposes of the processing;

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

- Description of the categories of data subjects;
- Description of the categories of personal data;
- Categories of recipients to whom the personal data may be disclosed (incl. recipients in third countries or international organisations);
- Transfers of personal data to a third country or an international organisation;
- Time limits for erasure of the different categories of data;
- General description of the technical and organizational security measures.

According to Rec. 82 GDPR the purpose of the records is twofold: they allow controllers to demonstrate compliance with the Regulation requirements as well as to fulfil their cooperation obligation by making records available, upon request by the supervisory authority. According to some studies[77], the records hold a third, substantially important role, namely assisting data controllers in the fulfilment of their obligation to satisfy data subjects' information requests.

Art. 30, para. 5 GDPR provides for an exemption to the general obligation to maintain records for processing activities. The exemption applies to enterprises or organisations with less than 250 employees. This quantitative criterion is introduced with view to the financial and organisational capacities of small-sized organisations which in most cases could not bear the costly and time-consuming burden of the record maintenance and administration.

The exemption is not unconditional. There are several hypotheses which significantly reduce its applicability. Should any of them arise, the obligation to maintain record of processing activities remains, regardless of the size of the organisation and the number of persons it employs.

First of all, keeping a record of processing activities is mandatory in case the processing is likely to result in a risk to the rights and freedoms of data subjects. As unclear as this condition may be, it refers to the general idea of the legislator to include as many activities as possible under the scope of the data

[77] Voigt P. and von dem Bussche A., *"The EU General Data Protection Regulation (GDPR). A Practical Guide"*, Springer International Publishing AG 2017, p. 44

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

protection legislation. This particular condition should be interpreted as to cover all data processing activities except for those which clearly bear a very minor risk to the rights and freedoms of data subjects. In all other hypothesis, keeping a record of processing activities is mandatory.

Record of processing activities should also be kept by organisations performing processing which is not occasional. Occasional processing or processing occurring for a very short period of time is not covered by this condition and, should such processing occur, the exemption applies. Nonetheless, as in practice occasional or temporary/short-in-time processing is very rare, this exemption condition would virtually be inapplicable, and organizations would need, in fact, to keep a record.

Lastly, the requirement to maintain records applies to processing of special categories of data (as per the meaning of Art. 9, para. 1 GDPR) or of data relating to criminal convictions and offences (as per Art. 10 GDPR). The amount of such sensitive data being processed is irrelevant to the application of this condition – as long as the organisation processes any such data, it is required to maintain a record. This condition significantly reduces the applicability of the exemption as virtually every organisation administrating HR-related information, processes some sensitive data (such as medical certificates, certificate for lack of criminal convictions, etc.).

As one or several of the above hypothesis apply to nearly any data processing, the applicability of the exception to the requirement for keeping a record of processing activities is very questionable. Taking into account the high amount of the fine which may be imposed for violation of that requirement (up to EUR 10 000 000 or 2% of the total worldwide annual turnover of the organisation; Art. 83, para. 4 GDPR), it is reasonable to suggest that every data controller should maintain a record irrespective of the size of its organisation.

- Legal practitioners are advised to maintain records, even though in most cases they may have less than 250 employees, as the personal information of clients they process may be classified as posing a high risk to their rights and could fall under the scope of special categories of data under Art. 9 or Art. 10. Furthermore, except in narrow cases, the processing executed by legal practitioners is not occasional but rather frequent. Therefore, it is highly recommended for them to keep records of processing activities. For instance, attorneys may have a record for all civil and labour contracts

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

concluded with the law firm employees.

7.1.3 Security of processing, Art. 32 (rec. 83)

The security of data is often seen as an important prerequisite for achieving compliance with data processing principles.[78] It is not a standalone requirement but rather a standard which should be embedded in all stages of data processing and respected throughout the whole life-cycle of data by both data controllers and data processors.

The obligation to keep and process data in a secure manner is established with Article 32 GDPR which requires data controllers and processors to implement appropriate technical and organisational measures to ensure the necessary level of security. The security obligation extends to the duty of data controllers and processors to ensure that persons acting under their authority shall process personal data solely under their instructions (Art. 32, para. 4 GDPR).

The infringement of this obligation is punishable with fines of up to EUR 10 000 000 or 2% of the total worldwide annual turnover of the respective organisation (Art. 83, para. 4 GDPR), which makes it one of the most significant principles established with the GDPR.

The security obligation requires the implementation of measures which would provide an adequate level of security to the processing. The legislator has not limited the scope of the measures leaving data controllers and processors with a choice of a great variety of measures available.

Nonetheless, Art. 32, para. 1 GDPR provides a list with minimum requirements which include:

- *Pseudonymisation and encryption of data* – these techniques are seen by the legislator as particularly effective for the purposes of data security; encryption is specifically referred to as an example of a measure to mitigate security risks (Recital 83 GDPR);

[78] Room S., *Security of Personal Data* in *European Data Protection Law and Practice*, IAPP publication, 2018, p. 169

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

- *Implementation of features allowing for ensuring the ongoing confidentiality, integrity, availability and resilience of processing systems and services* – these requirements target virtually all modern technology and IT systems which shall from now on commit to data security in an effective and durable manner;
- *Mechanisms permitting to restore the availability and access to personal data in a timely manner in the event of an incident* – such mechanisms may include regular back-up and emergency power supply; there is no definition of what is perceived as 'timely manner'; however, by analogy with organisations' report obligations in case of a data breach, the recovery of data should happen as soon as possible;
- *Processes for regular testing, assessing and evaluating the effectiveness of adopted measures, etc.* – as data security is not a one-time obligation but requires a continuous effort, this requirement refers to the need for a constant care and maintenance of implemented measures, which shall be regularly assessed and adapted over time.

Adherence to an approved code of conduct or an approved certification could be used to demonstrate compliance with the requirements regarding security of processing (Art. 32, para. 3 GDPR).

Article 32, para. 2 GDPR requires a risk-based approach for the purposes of the assessment of what measures would be appropriate. Data controllers and processors are thus obliged to carry out objective risks assessment in order to determine what measures are adequate to implement. Recital 83 GDPR further clarifies that for the purposes of data security risk assessment, consideration should be given to dangers such as accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed which may in particular lead to physical, material or non-material damage. The greater the dangers to personal data are, the more elaborated measures shall be implemented.

The risk-based approach also requires a consideration of the state-of-the-art and the cost of implementation of the measures. As data is increasingly processed in more and more sophisticated manners, the state-of-the-art test is introduced in order to oblige data controllers and processors to

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

consider the most recent and elaborated industry practices.[79] At the same time, a high cost of implementation may sufficiently deter the organization's efforts to mitigate security risks.

Examples of measures every data controller should implement are: keeping CVs and dossiers of the employees in cabinets/ premises with authorised access, internal policies on information security for the employees (i.e. regulating authorised access to and use of devices, introduction of clean desk policy, etc.). Legal practitioners should advise their clients on concrete technical and organisational measures they should take based on the specific categories of data they process and the risk for the data subjects' rights and interests.

7.1.4 Data Protection Impact Assessment (DPIA), Art. 35 (Recitals 84, 90-94)

Notion, requirement and content

The data protection impact assessment (DPIA), also known as privacy impact assessment, is a powerful instrument which can help organisations identify the most effective way to comply with data protection requirements. It allows for identification of potential risks, their evaluation and ultimately for mitigating those risks by implementing adequate technical and organisational measures. The DPIA is promoted by the ICO and other regulatory bodies as an integral part of taking a privacy by design approach. As the GDPR is built upon a general risk-based approach requiring processing operations to be evaluated in an objective case-by-case manner accounting for the relevant risks, DPIA is an irreplaceable ally to data controllers in their efforts to identify and mitigate those risks.

Conducting a DPIA is not only an obligation but also an advantageous mechanism assisting data controllers in their efforts to ensure GDPR compliance, particularly where processing is likely to result in a high risk to individuals' rights and freedoms. Therefore, Art. 24 GDPR should be read in close conjunction with the provisions of Art. 35 GDPR establishing DPIA obligations.

Article 35, para. 1 GDPR establishes the requirement for the controller, to carry out an assessment of the impact of the envisaged processing on the protection of personal data. For the purposes of

[79] Room S., *Security of Personal Data* in *European Data Protection Law and Practice*, IAPP publication, 2018, p. 173

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

evaluating whether an assessment is needed, the controller shall take into account the nature, scope, context and purposes of the processing. Following the general risk-based approach adopted throughout the Regulation, the assessment shall be performed if the processing is likely to result in a high risk to the rights and freedoms of natural persons. A high risk is likely to occur in case of a use of new technology (Art. 35, para. 1 GDPR) or where processing operations are of a new kind and the controller has not yet carried out an impact assessment or such assessment becomes necessary due to the time elapsed since the initial processing (Rec. 89 GDPR).

Art. 35, para. 3 GDPR provides an indicative and not limitative list of risk-prone situations to consider. A high risk is likely to occur, and a DPIA should be carried out in case of:

- A systematic and extensive evaluation of personal aspects of individuals based on automated processing, including profiling, in case decisions producing legal effects or affecting the individuals are based on this evaluation;
- Processing on a large scale, *i.e.* a considerable amount of personal data at regional, national or supranational level[80], of special categories of data referred to in Art. 9, para. 1 GDPR, or of personal data relating to criminal convictions and offences referred to in Art. 10 GDPR; or
- A systematic monitoring of a publicly accessible area on a large scale, especially when using optic-electronic devices or when it prevents data subjects from exercising a right or using a service or a contract (Recital 91 GDPR).

DPIA method

The DPIA should cover the whole life cycle of processing operations. At the same time a single assessment may address a set of similar processing operations that present similar high risks (Art. 35, para. 1 GDPR). The DPIA may thus have a large scope, covering more than one processing operation, but should acknowledge all aspects of those operations – from their conception to their consequences.

The DPIA should be carried out prior to the processing (Art. 35, para. 1 GDPR). This requirement is consistent with the privacy-by-design and privacy-by-default concepts. The DPIA could be an on-

[80] Rec. 91 GDPR

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

going process accompanying a developing processing activity and should be updated once the processing has actually started. In addition, in case of a change of the risk, it should be revised accordingly (Art. 35, para. 11 GDPR).

Art. 35, para. 7 GDPR establishes the minimum requirements for conducting the DPIA. They include:

- Systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;
- Assessment of the necessity and proportionality of the processing operations in relation to the purposes;
- Assessment of the risks to the rights and freedoms of data subjects; and
- Measures envisaged to:
    - Address the risks (safeguards, security measures and mechanisms to ensure protection of data);
    - Demonstrate compliance taking into account the rights and legitimate interests of data subjects and other persons concerned.

In case a DPO has been designated, his/her advice shall be sought by the controller in the process of carrying out a data protection impact assessment (Art. 35, para. 2 GDPR), particularly on the following topics[81]:

- Whether or not to carry out a DPIA;
- What methodology to follow when carrying out a DPIA;
- Whether to carry out the DPIA in-house or whether to outsource it;
- What safeguards (including technical and organisational measures) to apply to mitigate any risks to the rights and interests of the data subjects;

[81] According to the Article 29 Working Party, *Guidelines on Data Protection Officers ('DPOs')*, WP 243, p. 17

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

- Whether or not the impact assessment has been correctly carried out and whether its conclusions (whether or not to go ahead with the processing and what safeguards to apply) are in compliance with the GDPR.

Art. 35, para. 10 establishes the conditions for exemption of the obligation to conduct a DPIA. Such is not mandatory when:

- The processing has a legal basis in Union law or in the law of the Member State to which the controller is subject,
- The said law regulates the specific processing operations, and
- A general impact assessment has already been carried out in the context of the adoption of that legal basis.

  Some specific situations are expressly excluded from the obligation for conducting a DPIA, namely where the processing concerns personal data from patients or clients by a single physician, other health care professional or lawyer. In such cases, a data protection impact assessment is not mandatory (Recital 91 GDPR).

7.1.5. Responsibility of the controller regarding the appointment of data processors (Art. 28, para. 1-3, Recital 81)

When entrusting a processor with processing activities, data controllers must observe a number of requirements. According to Art. 28, para. 1 GDPR controllers shall use only processors who provide sufficient guarantees for the implementation of appropriate technical and organisational measures for the purposes of respecting all GDPR obligations and ensuring protection of data subjects' rights. Recital 81 clarifies that processors selected by controllers to process data on their behalf should provide sufficient guarantees, in particular in terms of expert knowledge, reliability and resources, to implement technical and organisational measures, including for the security of processing.

The controller may use the processor's adherence to an approved code of conduct or an approved certification mechanism in order to demonstrate compliance with these requirements (Art. 28 para. 5

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

GDPR). The duty of the controller does not end there – he/ she is expected to continuously ascertain the processor's capacity to adhere to and respect the said measures.

Pursuant to Art. 28, para. 3 GDPR the processing by a processor shall be governed by a binding contract or another legal act, in any case concluded in writing, including in electronic form (Art. 28, para. 9 GDPR). The contract needs to contain at least the following information:

- Subject matter;
- Duration of the processing;
- The nature and purpose of the processing;
- The type of personal data which are processed;
- The categories of data subjects to whom the data relate; and
- The obligations and rights of the controller.

In addition to the following basic information, the contract shall stipulate in greater detail the obligations of the processor. Clauses introducing the processor's obligations must include in particular:

- Requirement to process the personal data only on documented instructions from the controller – providing these instructions in writing is not only a requirement, but also an advantage to both controller and processor as it allows them to effectively demonstrate compliance;
- Requirement to ensure that persons authorised to process personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;
- Requirement to take all technical and organisational measures for the purposes of data security;
- Requirement not to engage another processor without prior specific or general written authorisation of the controller. In case such general written authorisation is provided, the processor shall inform the controller of any intended changes regarding other processors, thereby giving the controller the opportunity to object to such changes;
- Requirement to ensure that, where applicable, other processors engaged by the processor are bound by and respect the same data protection obligations as those set out in the contract between the controller and the processor;

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

- Requirement to assist the controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights;
- Requirement to assist the controller in ensuring compliance with data security obligations, namely in terms of ensuring security of processing, notifying personal data breach to the supervisory authority, communicating personal data breach to the data subject, conducting DPIA and making prior consultations to the supervisory authority;
- Requirement to delete or return, at the choice of the controller, all the personal data to the controller after the end of the provision of services and to delete all existing copies of these data;
- Requirement to make available to the controller all information necessary to demonstrate compliance with the obligations relative to the possibility of engaging a processor. In the case of on-going legal consultancy, legal practitioners should explore all the relations between their clients and potential processors and make sure there are written contracts which comply with all the requirements prescribed by Art. 28, para 3.

When legal practitioners are in the role of controllers, they should likewise sign a written contract or other similar act, with the data processor – for example when using a cloud service, the could service provider acts as a processor.

7.1.6 Cooperation with data protection authorities, Art. 31 (Recital 82)

Pursuant to Art. 31 GDPR controllers and processors, and, where applicable, their representatives, shall cooperate with the supervisory authority in the performance of its tasks.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

The cooperation shall be performed upon request of the respective authority. Some authors suggest that, *a contrario*, the cooperation does not need to be voluntary or on the controller's initiative.[82] The general understanding is that requests of the supervisory authority, as per the meaning of the GDPR, are not administrative acts and therefore, no specific reason need to be provided to the controller. [83]

The provision of Art. 31 GDPR is fairly shortly worded. It is clarified and reinforced by other provisions which establish cooperation obligations in further details. For instance, Art. 30, para. 4 GDPR requires data controllers to make available to the supervisory authority records of processing activities. The lack of indications on the enforceability of the cooperation request is more perplex and translates in the conclusion that the cooperation obligation is not enforceable. Studies suggest that, in this case, cooperation requests of supervisory authorities will be governed by EU law and national laws of EU Member States.[84]

7.2. Technical obligations, Art. 25

While the organisational obligations, analysed under in Section 7.1. above, essentially confirm already well-established requirements, the legislator goes one step farther from the regime regulated by the Data Protection Directive, by imposing to data controllers new and explicitly formulated obligations in relation to the technical development of new processes and products.

Article 25 GDPR introduces the requirement for data controllers to ensure that both in the planning as well as in the implementing of new products or services involving processing of personal data appropriate technical and organisational measures are taken in order to guarantee the proper application of data protection principles and to integrate safeguards to data subjects' rights.

The provisions of Art. 25 GDPR represent a key innovation as they set up an explicit requirement for data controllers to take specific steps in terms of design and default implementation of data processing activities. Respect to data protection principles should from now on be guaranteed *ex post* and should

[82] Voigt P. and von dem Bussche A., *"The EU General Data Protection Regulation (GDPR). A Practical Guide"*, Springer International Publishing AG 2017, p. 37
[83] Ibid.
[84] Ibid.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

be treated as a key requirement to any foreseen planning or implementation of new product or services. The legislator has institutionalised the understanding that compliance with data protection principles cannot be achieved solely by regulatory measures, but it should be a key element of the design and functioning of any product or service involving processing of data.

The same requirement is introduced in Art. 20 of Directive 2016/680. Its wording is identical to the provisions of Art. 25, paras. 1 and 2 GDPR.

Infringements of the obligations of Art. 25 GDPR are punishable with fines of up to EUR 10 000 000 or 2% of the total worldwide annual turnover of the respective organisation. However, researchers have pointed out[85] that the provisions of Art. 25 are unclear and do not provide sufficient details on the technical and organisational measures required. These requirements would need to be further clarified and will most probably be subject to interpretation and shaping by legal practitioners and judges.

7.2.1 Data protection by design (Art. 25, para. 1, Recital 78)

Art. 25, para. 1 GDPR institutionalises the data protection-by-design concept by introducing the requirement for data controllers to take measures *designed* to implement data protection principles. Recital 78 GDPR further clarifies that when developing, designing, selecting and using applications, services and products involving processing of personal data, producers of products, services and applications should be encouraged to take into account data protection principles and, with due regard to the state of the art, to make sure that controllers and processors are able to fulfil their data protection obligations.

The above establishes the new understanding of how data protection should be viewed, implemented and enforced. It should not be perceived as an afterthought or a fix but needs to be considered at the very earliest stage of inventing, developing or selecting products, applications or services. Technological progress obliges a shift of the focus. The innovative regulatory approach now considers

[85] Voigt P., von dem Bussche A., *The EU general data protection regulation (GDPR). A practical guide*, Springer International Publishing, 2017, p. 64

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

the role of technologies in the data protection set-up. Compliance analysis shall be performed from this perspective.

Notion: strengthening and specification of the fundamental principles. Prevention of infringement

The data protection by design approach promotes data protection principles from the very beginning of any data processing activity.[86] It aims at empowering privacy and data protection and at ensuring their protection as today they are perceived as core values of democratic societies. The endeavour of employing technological mechanisms to guarantee implementation of data protection principles at the very beginning of the lifecycle of any activity or product involving data processing translates in the institutionalisation of the privacy by design concept.

Although the privacy by design requirement imposes a significant burden on data controllers obliging them to embed data protection compliance into their systems and tools, it is largely welcomed by practitioners and regulatory authorities. It is considered an essential tool helping data controllers comply with the rest of the GDPR requirements more easily and more effectively.

Data controllers are thus encouraged[87] to consider and employ the privacy by design principle when, for instance, they:

- Build up a new internal IT system or administrative tool;
- Develop policies, business processes or practices;
- Embark on an initiative or activity;
- Develop or create a new service or product and launch it on the market, and the said activity involves processing of personal data.

Employing the data protection by design approach is considered to be an irreplaceable tool for enhancing the prevention and minimising the risk of infringements. In its guidance paper on the

[86] ICO, *The Guide to Data Protection*, available at https://ico.org.uk/media/for-organisations/guide-to-data-protection-2-9.pdf
[87] Ibid, p. 128

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

GDPR, the British ICO points out[88] the following benefits directly streaming out from the data protection by design approach:

- Identification of issues and potential risks of violation of data protection principles at a very early stage. Thereby, simpler and less costly remedy measures.
- Increased general awareness of data protection principles and of their impact.
- Better compliance with data protection regulations;
- Lower risks of undertaking privacy intrusive actions with negative effect upon data subjects.

Application of privacy enhancing technology. Implementation options. Technical state-of-the-art

The privacy by design concept translates in the requirement to embed privacy mechanisms into technology. Such technologies are commonly known as Privacy-Enhancing Technologies (PETs). There is no uniform definition of PETs, but they generally refer to *the use of technology to help achieve compliance with data protection legislation*.[89]

Examples across different privacy and data protection studies include encryption, metadata and digital rights management, protocols for anonymous communications, application programming attribute-based credentials, user interface, identity management, architecture and private search of databases. The GDPR itself provides explicit examples of techniques for implementing privacy by design measures, namely timely pseudonymisation of personal data and systems directed towards data minimisation.

Application of PETs guarantees higher protection of personal data of individuals, and thereby, of their rights, but also serves as a shield to corporate confidential information. The implementation options of such measures may be coordinated and evaluated with the assistance of, where present, the DPO. When implementing data protection by design measures regard should be given to the technical state of the art. Although the concept of data protection by design is explicitly introduced through the

[88] Ibid, p. 128
[89] Kenny S, *An Introduction to Privacy Enhancing Technologies*, IAPP, The privacy advisor, available at https://iapp.org/news/a/2008-05-introduction-to-privacy-enhancing-technologies/

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

provisions of the GDPR, after years of debate and struggle, in order to guarantee that data protection regulations keep up with the pace of technological developments, the provisions of the Data Protection Directive also acknowledged the importance of the technical state of the art and the cost of implementation of security measures. In its Art. 17 it read *"[h]aving regard to the state of the art and the cost of [...] implementation, [technical and organisational] measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data."* Thus, here nothing new - measures should correspond to the current stage of technological progress and reflect the costs of implementation.

Reasonableness of measures. Balancing of interests

The implementation of privacy mechanisms into technology is not a simple task. It requires a careful study of the balance between the features of the developed product/service and the measures which may be taken with view to data protection requirements. Studies show[90] that sometimes the two may come into conflict with other functional or regulatory requirements.

Therefore, the provisions of Art. 25, para. 1 recognise the need to take into account a number of criteria when assessing the necessary implementation of technical measures and data protection by design features. Apart from the technological state of the art discussed above, relevant circumstances include the nature, scope, context and purposes of processing, the cost of implementation of the relevant measures as well as the risks for the rights and freedoms of natural persons posed by the processing. All these circumstances should be weighted out and considered in order to establish a level of reasonableness of the technical measures which could be implemented.

7.2.2. Data protection by default (Art. 25, para. 2)

The concept of data protection by default is another innovation GDPR introduces. Up until now the Data Protection Directive did not contain explicit reference to such notion and requirements related thereto. Art. 25, para. 2 GDPR now establishes the requirement for data controllers to implement

[90] EU Agency for Network and Information Security, *Privacy and Data Protection by Design*, December 2014, p. 11

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

appropriate technical and organisational measures ensuring that, by default, only personal data strictly necessary to the relevant processing purpose are processed.

The reason behind this conceptual modernisation is rooted in the resolution to protect data subjects against the widespread practices of data controllers to collect as much data as possible. As of 25th of May 2018, only personal data which are strictly necessary to the processing shall be obtained. The data protection by default concept and the requirements related thereto strengthen the principle of data minimization and aim at fixing several other issues in the context of data protection.

Notion: Remedy against the "privacy paradox". Strengthening of the principle of data minimisation

The requirements of with Art. 25, para. 2 GDPR imposing data protection by default obligations to data controllers are assigned with a particularly important role – to solve the so-called privacy paradox.

According to researchers, the privacy paradox refers to the phenomenon where data subjects feel uncomfortable giving away personal information, yet they increasingly and uncontrollably keep sharing it.[91] Users are rarely aware of privacy policies and conditions under which their data is being processed. As information has an important monetary and competitive value, up until now the tendency was clear – the more data is being collected and processed, the better. The concept of data protection by default shifts the current setting and requires data controllers to implement such technical and organisational measures so as to ensure that default settings are as much privacy friendly as possible without the need for data subjects to have to change them in order to protect their data. Should data subjects wish to allow further use of personal information or share additional data, they may change their privacy settings and opt in to the respective data processing. This new perspective aims at protecting less technically advised users who are not aware of the amount of personal data which is shared by default by the products/services they use and who do not have the sufficient knowledge to change the relevant privacy settings.

[91] Zomorodi M, Poyant J, Aaron K, *Privacy Paradox: What You Can Do About Your Data Right Now*, available at: https://www.npr.org/sections/alltechconsidered/2017/01/30/512434746/privacy-paradox-what-you-can-do-about-your-data-right-now

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

In addition, data protection by default measures are deemed to ultimately decrease the amount of data which is collected and processed by default by various products/services. In line with the data minimisation principle, they should lessen the amount of personal data collected, the extent of processing, the storage periods as well as the data accessibility.

Scope of the obligation

Data protection by default measures require a proactive approach. While design measures should be considered and embedded at the beginning of the lifecycle of a service or a product, the data protection by default methods may be implemented throughout the processing activities. Nevertheless, in order to ensure the possibility of implementing data protection by default techniques, such capabilities should be considered at the design stage of the development of a product/service. In a sense, it may be accepted that data protection by default is a part of the data protection by design set-up.[92]

The general understanding is that pseudonymisation and anonymisation are techniques which satisfy the requirements of Art. 25 GDPR. The data minimisation principle shall be followed throughout their implementation. Pursuant to Art. 25, para. 2 GDPR privacy friendly default settings should apply "*to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility*" ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed.

7.2.3. Certification with indicative effect for legal practitioners (Art. 25, para. 3)

Means to demonstrate compliance with the requirements of Art. 25 GDPR is an important aspect of the fulfilment of these obligations. Having in mind the high amount of the fines which may be imposed for violation of these provisions, such means have key role both for data controllers/processors/developers, as well as -for Supervisory Authorities.

[92] According to Ann Cavoukian. See Hansen M, *Data Protection by Default – Requirements, Solutions, Questions*, IPEN Workshop, Vienna, 9 June 2017, p. 4, available at: https://edps.europa.eu/sites/edp/files/publication/17-06-09_marit_hansen-dataprotectionbydefault_ipen-workshop_vienna_hansen_en.pdf

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

Article 25, para. 3 provides for such means. It establishes the possibility to use an approved certification mechanism (as per the terms of Art. 42 GDPR) in order to demonstrate compliance with data protection by design and data protection by default obligations.

The certification requires adherence by controllers/processors to established data protection certification mechanisms and use of data protection seals and marks. It is voluntary and available through transparent process. The ultimate aim is to be able to ensure a certain level of compliance. Notwithstanding, data controllers/processors are bound by all relevant GDPR requirements and their responsibility is in no way reduced merely on the grounds of existing certification. The effect of the certification thus remains indicative to legal practitioners and judges when they are faced with compliance assessment regarding Art. 25 obligations.

7.3. The role of the data protection officer

The institutionalisation of the data protection officer (DPO) is a key innovation of the GDPR. Article 37 of the Regulation lays down the cases where the designation of a DPO is mandatory.

The requirement to appoint a DPO may apply to both the data controller and the data processor.

The risk-based approach and philosophy adopted throughout the GDPR is followed in Art. 37 and following. The requirement to appoint a DPO is not connected to quantitative criteria such as number of employees of data controllers but relates to the nature of data processing activities carried out by them and the risks to data subjects' rights throughout these activities.

Article 37, para. 1, lit. a GDPR establishes the requirement for public authorities or bodies to appoint a DPO, except for courts acting in their judicial capacity. The GDPR does not provide further clarification of what is considered public authority or body. The understanding of the Article 29 Working party is that the notion is to be determined under respective national law.[93] Definitions would normally include national, regional and local authorities as well as a range of other bodies governed by public law.

[93] Article 29 Working Party, *Guidelines on Data Protection Officers ('DPOs')*, WP243 rev.01, p. 6

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

Art. 37, para. 1, lit. a GDPR provides for an exception to the mandatory designation of a DPO. The exception applies to *courts or independent judicial authorities when acting in their judicial capacity* (Recital 97 GDPR). The idea behind this exception refers to the general understanding of judicial independence, confirmed with Art. 55, para. 3 and Recital 20 GDPR, establishing the competence of supervisory authorities. According to this provision, compliance of personal data processing performed by courts acting in their judicial capacity should be enforced through a separate regime in order to safeguard the independence of the judiciary in the performance of its judicial tasks, including decision-making. Supervision of data processing operations performed by courts acting in their judicial capacity should be entrusted to specific bodies within the judicial systems of Member States, which will *ensure compliance with the rules of this Regulation, enhance awareness among members of the judiciary of their obligations under this Regulation and handle complaints in relation to such data processing operations.*

The provisions regarding DPO designation follow the same logic and exclude courts and other independent judicial authorities acting in their judicial capacity from the mandatory requirement to appoint a DPO. At the same time the GDPR does not provide a definition of "judicial capacity". This lack of precision could create confusion as to when a DPO is to be appointed by courts and independent judicial authorities. Moreover, as not all data processing activities undertaken by a court fall within the scope of the judicial capacity of the court. Sometimes it will be difficult to separate, and therefore supervise those data processing operations that border with the judicial capacity.

Notwithstanding, the provisions of Art. 37, para. 1, lit. a GDPR apply and DPO designation is mandatory with regard to legal practitioners in the public sector.

Article 37, para. 1, lit. b and c GDPR apply to data controllers/processors in the private sector. Pursuant to Art. 37, para. 1, lit. b GDPR the appointment of a DPO is mandatory if the core activities of the data controller, by virtue of their nature, their scope and/or their purposes involve regular and systematic monitoring of individuals on a large scale. On the other hand, Art. 37, para. 1, lit. c GDPR stipulates that the designation of DPO is mandatory where the core activities of the data controller involve processing on a large scale of special categories of data or personal data relating to criminal convictions and offences.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

The GDPR does not provide clear definitions of the concepts engaged in Art. 37, para. 1, lit. b and c GDPR. Both provisions refer to the *"core activities of the controller or processor"*. According to the clarification brought by Recital 97 core activities relate to the primary activities and not to the processing of personal data as ancillary activity. Employee payment and internal IT support activities are considered such ancillary activities.[94]

The term "large scale" also requires attention as Art. 37, para. 1 GDPR does not clarify its meaning. Although it refers to data protection impact assessments, Recital 91 GDPR provides some guidance on the Art. 37 terminology stipulating that *"large-scale processing operations [...] aim to process a considerable amount of personal data at regional, national or supranational level and [...] could affect a large number of data subjects [...] likely to result in a high risk [...] to the rights and freedoms of data subjects"*. Even with these clarifications in mind, in the absence of clear quantitative criteria, it may currently be difficult to establish whether a processing is carried out on a large scale. This analysis would be subject to interpretation and may evolve with the help of legal practitioners and judges. According to the Article 29 Working Party the following criteria should be considered when determining whether the processing is carried out on a large scale: the number of data subjects concerned (a number or a proportion); the volume of processed data; the duration or permanence of data processing; the geographical extend of the processing.

The reference to "regular and systematic monitoring' used in Art. 37, para. 1, lit. b GDPR is not explained throughout the provisions of the GDPR. However, Recital 24 GDPR provides some information stating that *"[i]n order to determine whether a processing activity can be considered to monitor the behaviour of data subjects, it should be ascertained whether natural persons are tracked on the internet including potential subsequent use of personal data processing techniques [such as] profiling [...] particularly in order to take [...] decisions for analysing or predicting [...] personal preferences, behaviours and attitudes."* With this in mind, the Article 29 Working Party interprets[95] the term "regular" to involve processing which is *"ongoing or recurring at particular intervals; repeated at fixed times; or constantly or periodically taking place"* and suggests[96] that

[94] Ibid., p. 7
[95] Ibid., p. 8
[96] Ibid., p. 9

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

"systematic" means *"occurring according to a system; pre-arranged, organised or methodical; taking place as part of a general plan for data collection; or carried out as a part of a strategy"*. According to the doctrine and recent research, customers loyalty programs, behavioural advertising and similar profiling activities are considered to involve a 'regular and systematic monitoring' and may lead to an obligation to appoint a DPO.

Art. 37, para. 1, lit. c GDPR requires a mandatory designation of a DPO in case the controller processes special categories of data pursuant to the meaning of Art. 9 GDPR and personal data relating to criminal convictions and offences as per the meaning of Art. 10 GDPR. The Article 29 Working Party has correctly noticed that although the quoted provision employs the word "and", there is no reason as to why the two case scenarios should be applied simultaneously.[97] Thus, a DPO is to be appointed in case where any of these types of processing is carried out.

Regarding the reflections around the DPIA, the GDPR stipulates that individual lawyers do not process "on a large scale" in general[98]. As stated in section 7.1.4, it is unclear if this exception applies to law firms, but most probably it will not and some of them might be obliged to appoint a DPO. According to The Law Society's guide, some law firms are more likely to be processing special categories of data, e.g. concerning health, ethnicity, political or religious beliefs, trade union membership, or sexual orientation of the firm's clients, or personal information relating to clients' criminal convictions and offences, and such processing might be conducted on a large scale[99]. An assessment should be made in all cases. Legal practitioners should pay attention to the national legislation that may oblige them to appoint a DPO in all cases or in different cases than the ones explicitly listed in Art. 37 GDPR. Unless it is clearly obvious that a mandatory designation of a DPO is not required, the Working Party under Article 29 recommends[100] that organisations carefully document the analysis carried out for determining whether or not a DPO is to be appointed. Such

[97] Ibid.
[98] See Recital 91.
[99] *The Law Society, Appointment of data protection officers by law firms. General Data Protection Regulation guidance, 2018, p. 6*
[100] Ibid., p. 5

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

documenting is considered needed for the purposes of demonstrating compliance with the accountability principle.

According to Art. 37, para. 5 GDPR the DPO shall be designated on the basis of professional qualities and expert knowledge of data protection law and practices as well as of the ability to fulfil the statutory responsibilities. The evaluation of a candidate's capabilities should refer to the specific processing activities carried out by the controller. According to German jurisprudence, the candidate's professional qualities are determined by the aggregate of their legal, organisational and technical knowledge.[101]

Paragraph 6 of Art. 37 GDPR allows for a choice between in-house and external DPO. The internal DPO may be an employee of the controller/processor, whilst the external DPO fulfils the tasks on the basis of a service contract. The service contract is by its very nature limited in time. With regard to that, a conclusion may be drawn that the DPO could be appointed for a limited period of time. Nevertheless, in order to ensure continuity and effective supervision of data processing activities, it may be advisable to designate a DPO for a period of at least two years. This requirement was part of the initial Commission proposal for the GDPR.[102] Although it did not make the final version of the draft, a period of at least two years seems reasonable in view of ensuring independence of the DPO and securing a certain level of efficiency of the DPO's work towards compliance with data protection principles.

Another organisational choice offered by Art. 37 GDPR refers to the possibility for a group of companies to appoint a single DPO (Art. 37, para. 2 GDPR) provided that the latter is easily accessible from each establishment. The accessibility requirement translates into the necessity to satisfy the following conditions:

[101] Voigt P. and von dem Bussche A., *"The EU General Data Protection Regulation (GDPR). A Practical Guide"*, Springer International Publishing AG 2017, p. 57

[102] Art. 35 of Commission Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data, COM (2012) 11 final; 2012/0011 (COD)

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

- The DPO should be available: The GDPR provisions do not require the DPO to necessarily be physically located on the same premises as the employees, but that he/she is available. According to the guidelines of the Article 29 Working party[103], the availability may be ensured e.g. through a dedicated contact form addressed to the DPO on the organisation's website, through a hotline or another secure means of communication.
- The DPO should be able to efficiently communicate with the data subjects and with the supervisory authority: According to the Article 29 Working party[104] , this requirement refers to the ability of the DPO to communicate with the data subject and the supervisory authority in the language used by them. In order to ensure communication in such a way, the Article 29 Working party clarifies, the DPO may be assisted by a team.
- The DPO contact details should be made available: Pursuant to Art. 37, para. 7 GDPR, the DPO contact details should be published as well as communicated to the relevant supervisory authority. According to the Article 29 Working party[105], the contact details of the DPO should allow data subjects (both inside and outside of the organisation) and the supervisory authority *to easily and directly contact the DPO without having to contact another part of the organisation*. The Working party considers the direct contact with the DPO to be an essential element of the secrecy/confidentiality which the DPO is bound by (Art. 38, para. 5 GDPR) and to thus have an important impact on the readiness of data subjects to complain to him/her.

7.3.1 DPO's involvement (Art. 38)

Art. 38 GDPR lays down the requirements for data controllers and processors regarding the performance of the DPO's role.

[103] Article 29 Working Party Guidelines on Data Protection Officers ('DPOs'), WP 243 rev.01
[104] Article 29 Working Party Guidelines on Data Protection Officers ('DPOs'), WP 243 rev.01
[105] Ibid.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

With regard to the DPO position, the controller needs to ensure that the DPO is involved, properly and in a timely manner, in all issues regarding the protection of personal data. (Art. 38, para. 1 GDPR). According to the Article 29 Working party's guidance, it is crucial that the DPO is made aware and involved at the earliest stage possible in all issues regarding personal data.[106] This is particularly relevant in terms of conducting DPIAs. Article 35, para. 2 GDPR sets out the explicit obligation for data controllers to seek advice of the DPOs for the purposes of conducting a DPIA. In addition, the Article 29 Working party explains that the early involvement of the DPO in issues regarding data processing is beneficial to demonstrating compliance with the privacy-by-design principle embedded throughout the Regulation.

The controller should provide the resources necessary to the DPO's tasks and access to personal data and processing operations and commit to maintaining his/her expert knowledge (Art. 38, para. 2 GDPR). According to various studies[107], this requirement means that the DPO should be granted a suitable work place, IT resources and maintenance, financial resources, specialist literature, administrative staff and sufficient time to fulfil his/her duties. Article 29 Working party adds that DPO access to personal data and processing operation should be guaranteed through an access to services such as Human Resources, legal, IT, security, etc.[108] Participation in workshops, seminars, courses, etc., encouraged by the controller, should give the DPO the opportunity to stay up to date with most recent developments in the field of data protection in order to increase his/her expertise. As already mentioned above, the necessary level of expertise should be determined in particular according to the data processing operations carried out by the controller (Recital 97 GDPR).

The DPO's independence should also be guaranteed and this is due whether or not he/she is an employee of the controller.[109] The controller needs to ensure that the DPO fulfils his/her tasks in an independent manner without receiving any instructions, and that he/she reports directly to the highest management level of the organisation (Art. 38, para. 3 GDPR). The direct reporting to the high

[106] Article 29 Data Protection Working Party, Guidelines on Data Protection Officers ('DPOs'), WP243 rev.01, p. 13
[107] Voigt P. and von dem Bussche A., *"The EU General Data Protection Regulation (GDPR). A Practical Guide"*, p. 59
[108] Article 29 Data Protection Working Party, Guidelines on Data Protection Officers ('DPOs'), WP243 rev.01, p. 14
[109] Recital 97 GDPR

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

management bodies should ensure that these bodies are aware of the DPO recommendations and advice.[110] However, this necessity should not be interpreted as to require the DPO to report every daily routine to the highest management level.

The DPO shall not be dismissed or penalised by the controller for performing his/her tasks. This requirement, introduced with Art. 38, para. 3 GDPR, reiterates the DPO independence obligation. Such penalties include absence or delay of promotion, prevention form career advancement, denial from benefits that other employees receive, etc.[111] It should be borne in mind that the prohibition of penalties relates exclusively to the DPO's tasks in this capacity.

Data subjects should be able to contact the DPO with regard to all issues related to processing of their personal data and to the exercise of their rights. In addition to this role, assigned by the provisions of Art. 38, para. 4 GDPR, the DPO should also be a contact point for supervisory authorities (Art. 39, para. 1 GDPR).

Pursuant to Art. 38, para. 5 GDPR the DPO is bound by secrecy or confidentiality in the performance of his/her tasks, according to EU or EU Member State law. The GDPR does not introduce special conditions regarding the confidentiality requirement, but rather refers to pre-existing EU legislation.[112]

Finally, the controller shall ensure that the tasks and duties which the DPO fulfils apart of those relating to the protection of personal data, do not result in a conflict of interests. This means that the DPO may perform other functions, as long as these functions do not give rise to conflicts of interest. According to Article 29 Working party guidance the DPO should not fulfil task leading him/her into determining purposes and means of personal data processing. Position entailing the fulfilment of such tasks include chief executive, chief operating, chief financial, chief medical officer, head of marketing, head of IT or head of HR.[113]

[110] Article 29 Working Party, Guidelines on Data Protection Officers ('DPOs'), WP243 rev.01, p. 15
[111] Ibid.
[112] Voigt P. and von dem Bussche A., *"The EU General Data Protection Regulation (GDPR). A Practical Guide"*, p. 59
[113] Article 29 Working Party, Guidelines on Data Protection Officers ('DPOs'), WP243 rev.01, p. 16

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

7.4. Reporting obligations

In order to increase transparency, the GDPR introduces a general reporting obligation in case of a data breach. In accordance with this obligation data breaches should be notified to the relevant supervisory authority as well as to the data subjects.

7.4.1 Reporting data breach to DPA, Art. 33 (Recital 73, 85-88)

Pursuant to Art. 33 GDPR, in case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours from the moment they became aware of it, notify the event to the competent supervisory authority.

According to the definition provided by Art. 4, No. 12 GDPR, "personal data breach" means "*a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed*". The reason for the breach is irrelevant. As long as a breach of security related to the processing of personal data occurs, it shall be reported. If the controller fails to fulfil this obligation, a fine may be imposed of up to EUR 10 000 000 or 2% of the total worldwide annual turnover of the organisation (Art. 83, para. 4 GDPR).

Article 33 GDPR is particularly focused on the notification periods which need to be respected. First of all, the reporting obligation is linked to the moment the controller becomes aware of it. However, it is not specified what is the appropriate timeframe for the controller to become aware of a data breach. Some authors suggest that the correct interpretation of that requirement is closely related to the risk-based approach adopted throughout the Regulation: the higher the possible data processing risks, the faster the controller should have become aware of an eventual breach.[114]

Further, according to Art. 33 GDPR, after having become aware of the data breach, the controller shall report it without undue delay and, where feasible, not later than 72 hours afterwards. The expression "where feasible" reveals the acknowledgment of the legislator that there might be reasons

[114] Voigt P. and von dem Bussche A., "The EU General Data Protection Regulation (GDPR). A Practical Guide", Springer International Publishing AG 2017, p. 66

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

interfering with the controller's ability to respect the 72-hour period. In those cases, the notification to the data protection authority should be accompanied by reasons for the delay. Nevertheless, even if the breach has been reported not later than 72 hours after the controller were aware of it, it might still be that the notification was not made without undue delay. Here again, a risk-based evaluation shall be carried out. Should the risks to the rights and freedoms of individuals be high, and the gravity of the breach be important, the immediacy shall be observed closely and considered more carefully. It would never be appropriate for a controller to purposely delay the notification until the last moment of the 72-hour notification period, just because they could.

Art. 33, para. 3 GDPR set out the formal requirements of the notification. It should contain at least the following information:

- The nature of the personal data breach, including where possible, the categories and approximate number of data subjects and of personal data records concerned;
- The name and contact details of the DPO or other contact person;
- The likely consequences of the personal data breach;
- The measures taken or proposed to be taken by the controller to address the breach and its possible adverse effects.

If the information above is not available at the same time, it is possible to provide it to the supervisory authority in phases (Art. 33, para. 4 GDPR). The immediacy of the notification is therefore of a higher importance, compared to the completeness of the notification, the latter being able to be supplemented at a later stage.

In addition to the notification obligation, and in line with the accountability principle, the controller is required to document any personal data breaches, including the facts relating to that breach, its effects and the remedy actions taken (Art. 33, para. 5 GDPR). This document would enable the controller to demonstrate compliance with the notification obligation.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

Article 33, para. 1 GDPR introduces one exception to the data breach notification to the supervisory authority. Such is not required in case the breach **is unlikely** to result in a risk to the rights and freedoms of natural persons. Recital 85 provides a list of risks which may result from a personal data breach, namely: *physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned.* It appears from these provisions that the risk does not need to be high in order for the obligation of notification to the DPA to arise.

Because of the specificities of legal practitioner's activities, they may always be obliged to notify the DPA in case of data breach.

7.4.2. Notifying data breaches to affected data subjects (Art. 34, Recital 73, 86-88)

In addition to reporting data breaches to the competent DPA, controllers are required to communicate, without undue delay, the affected data subjects in case the breach is likely to result in a high risk to their rights and freedoms (Art. 34, para. 1 GDPR). The language used for the notification shall be clear and plain in order to allow data subject to understand the information and to take necessary precautions (Recital 86 GDPR). The notification should describe the nature of the data breach as well as provide at least the following information:

- The name and contact details of the DPO or other contact person;
- The likely consequences of the personal data breach;
- The measures taken or proposed to be taken by the controller to address the breach and its possible adverse effects.

Art. 34, para. 3 GDPR provides for an exemption to the notification obligation, listing three alternative conditions at least one of which shall be met:

- The controller has implemented appropriate technical and organisational measures, such as encryption, and those measures were applied to the personal data affected by the breach; or

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

- The controller has taken subsequent measures ensuring that the high risk to the rights and freedoms of individuals is no longer likely to occur; or
- The notification would involve disproportionate effort, in which case a public communication should be held informing data subjects on the breach in an equally effective manner.

Responses and reactions to data breach shall be carried out in close coordination with the competent supervisory authority. The DPA may require from data controller to notify the breach to affected data subjects in case it establishes that a high risk to their rights and freedoms exists. The DPA may also hold that an exemption condition is met, and the notification is therefore not mandatory (Art. 34, para. 4 GDPR).

Chapter 8: Awareness and guarantee of the rights of the data subject

All data subject's rights have been thoroughly examined within this section, as legal practitioners need to have sufficient and adequate knowledge of the matter when advocating for the rights of their clients, who might be data subjects as well.

8.1. Transparent information, communication and modalities for the exercise of the rights of the data subject (Art. 12)

Transparency is a key obligation laid down by GDPR applicable to a number of cases to ensure the high level of personal data protection. Transparency is a relevant obligation in view of guaranteeing the fair processing of personal data (Art. 13-14). It is likewise an important obligation regulating the manner of communication of controllers and data subject's rights (Art. 15-22, Art. 34). Moreover, transparency must be respected by controllers facilitating the exercise of data subject rights (Art. 15-22)[115]. Furthermore, in order to demonstrate compliance with the principle of accountability, the controller must execute processing activities in a transparent manner. It should be noted that

[115] Article 29 Working party, Guidelines on transparency under Regulation 2016/679, WP260, p. 5.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

transparency as obligation should be observed by the data controller regardless of the legal basis of the processing[116]. It should be stressed that when construing the provisions regarding data subject rights, the transparency obligation should be always taken into account as it provides guidance as how data subject rights must be exercised.

In particular, Art. 12 regulates the fashion of information provision to data subjects – the controller must take the necessary measure to ensure that all relevant information is available to the data subject in *concise, transparent, intelligible and easily accessible form, using clear and plain language*. The respect of this obligation is in particularly important in case the respective data subject is a child (Art. 12, para. 1). The regulation stipulates that the information should be provided in writing or in other means, also stating the possibility to provide the requested information in a digital format (i.e. Privacy Policy on a website). Information could be provided orally to data subject as well but only on the condition that he/ she has requested such and that the identity of the data subject concerned could be proven by other means. Furthermore, the controller should provide the information to the data subject free of charge (Art. 12, para. 5).

- In the light of legal practitioners GDPR interpretation and application, it should be noted that every time the controller uses ambiguous language or strictly technical terminology, or the information of a processing operation is not easily accessible to data subjects, the controller acts in violation of the GDPR.

The Article 29 Working Party gives examples for techniques that could be used for compliance with the transparency requirement[117]:
- For digital environment: layered privacy statements/ notices and - "Push" and "pull" notices management, transparency dashboards and "learn more" tutorials.
- Hard copy/ paper environment, for example when entering into contracts by postal means: written explanations, leaflets, information in contractual documentation and others;

[116] Ibid., p. 6.
[117] For further information check Article 29 Working Party, Guidelines on transparency under Regulation 2016/679,

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

- Telephonic environment: oral explanations by a real person, automated or pre-recorded information with options to hear more detailed information;
- Screenless smart technology/ IoT environment such as Wi-Fi tracking analytics: icons, QR codes, voice alerts, written information on the smart device, messages sent by SMS or email and others;
- Person to person environment, such as responding to opinion polls, registering in person for a service: oral explanations, written explanations provided in hard or soft copy format;
- "Real-life" environment with CCTV/ drone recording: visible boards containing the information, public signage, public information campaigns, newspaper/ media notices.

For legal practitioners' suitable measures may be:

- a privacy notice on the site;
- a special notice if the site contains a form/questionnaire to be filled by natural persons;
- a concise and easy to understand policy regarding the processing of personal data of clients on the site and on paper in the legal practitioners' offices that can be read by clients and other natural persons.

8.2. Information to be provided where personal data are collected from the data subject. Information to be provided where personal data have not been obtained from the data subject (Art. 13-14)

Articles 13 and 14 of GDPR further outline the items of information that must be provided to the data subject. Firstly, information about the controller's identity including his/ her contact information regardless whether the data has been collected directly from the data subject or not (Art. 13, para. 1, lit. a, Art. 14, para. 1, lit. a) Further, if the controller has appointed a DPO their contact details should be likewise available to the data subjects concerned (Art. 13, para. 1, lit. b, Art. 14, para. 1, lit. b). The data subject should also be aware of the purposes of processing and their foundation in law – Art. 13, para. 1, lit. c, Art. 14, para. 1, lit. c. If the personal data concerned is processed on the basis of the

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

legitimate interest of the controller, this legitimate interest should be made clear to data subjects (Art. 13, para. 1, lit. d, Art. 14, para. 1, lit. b). Quite logically, in the case where personal data is directly collected from an individual, it is not required that the provider discloses the type of data that is to be processed. However, when data is not directly obtained from a data subject, and yet the controller processes personal data, then the controller has to disclose which categories of personal data are being processed – Art. 14, para. 1, lit. d. Additionally, data subjects must be aware of the identity of the possible recipients of the data. The provisions of Art. 13, para. 1, lit. e and Art. 14, para. 1, lit. e should be construed in juncture with the provision of Art. 4, No. 9 which provides for the legal definition of the term "recipient". Hence, it should be underlined here that not only third parties are to be considered recipients of data, but processors and joint controllers (if applicable) to whom data is disclosed also fall under the "recipient" definition. In this relation, in order for the controller to demonstrate that personal data is processed in accordance with the fairness principle[118] and to comply with the transparency obligation, he/ she must be able to precisely determine the identity of the recipients[119]. If the controller chooses to disclose only the categories of the data recipients, he/ she should be able to demonstrate how this is compatible with the principle of fairness. Furthermore, the controller should be as specific as possible defining the different categories of data recipients (if applicable). When intending to transfer personal data to a third country or international organization, the controller is obliged to inform the data subjects about this intention and the existence or absence of an adequacy decision by the Commission, or in the case of some kinds of transfers, reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available (Art. 13, para. 1, lit. f, Art. 14, para. 1, lit. f).

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

1) the period for which the personal data will be stored, or the criteria used to determine that period;
2) the existence of the right to request from the controller access to and rectification or erasure

[118] For further information of data processing principles, please see the Annex to the current report.
[119] Article 29 Working party, Guidelines on transparency under Regulation 2016/679, WP260, p. 32.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability;

3) where the processing is based on lit. a of Art. 6, para. 1 or lit. a of Art. 9, para. 2, the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;
4) the right to lodge a complaint with a supervisory authority;
5) the existence of automated decision-making, including profiling, 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.

When the data was not obtained from the data subject, the data controller should provide her or his source and, in a case where the processing is based on the legitimate interests of the controller or a third party, what are these interests. Where the origin of the personal data cannot be provided to the data subject because various sources have been used, general information should be provided (Recital 61). If the data subject provided the data, the controller should inform him of her whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether he or she is obliged to provide the personal data and of the possible consequences of failure to provide such data.

In certain cases, the right to request information is limited. When the data are acquired from the data subject, the only limitation is when he or she already has the information (Art. 13, para. 4). When the data are not obtained from the subject, there are more limitations (Art. 14, para. 5):

- when the data subject already has the information;
- when the provision of such information proves to be impossible, would involve a disproportionate effort or would make the achievement of the objectives of the processing impossible or seriously impair them;

An example of impossibility to provide information would be when the controller does not have any means to contact the data subject. According to the Article 29 Working Party, the impossibility must be directly connected to the fact that the personal data was not obtained from the data

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

subject[120].

Where a data controller seeks to rely on the exception for disproportionate effort, it should assess the effort involved for the data controller to provide the information against the impact on the data subject if he or she was not provided with the information. This assessment should be documented by the data controller in accordance with its accountability obligations. The Working party also states that these exceptions cannot be routinely relied upon by data controllers who are not processing personal data for the purposes of archiving in the public interest, for scientific or historical research purposes or statistical purposes[121];

- when the exercising of the right might impair the achievement of the objectives of that processing.

An example of impairment could be a bank required to report suspicious activity relating to accounts held with it under anti-money laundering legislation.

- when the obtaining or disclosure is expressly laid down by EU or EU Member State law;
- when an obligation of professional secrecy regulated by EU or EU Member State law applies – this will be the case with the legal professional privilege.

According to the Article 29 Working Party[122], these limitations should, as a general rule, be interpreted and applied narrowly.

The controller may refuse to provide information if requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, see Art. 12, para. 5. In this case the controller has two options: 1) charge a reasonable fee taking into account the administrative costs or 2) refuse to act on the request.

If the controller intends to process the personal data for a new purpose, different than the ones for which they were collected, he or she should provide the data subject with information on that new purpose before processing. It could be useful when obtaining the data to inform data subjects for eventual future processing, if it is likely it will be conducted given the activity of the controller.

[120] Article 29 Working party, Guidelines on transparency under Regulation 2016/679, WP260, p. 27
[121] Ibid
[122] Ibid, p. 25

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

8.3. Right of access by the data subject, Art. 15

While the obligations of the controller under Art. 13 and 14 must be fulfilled without any actions on the side of the data subjects, the right to access could be exercised after filing a request. Data subjects have the right to know if their information is being processed by the controller and if so:

1) the purposes of the processing;
2) the categories of personal data concerned;
3) the recipients or categories of recipients, in particular recipients in third countries or international organisations;
4) the envisaged period for which the personal data will be stored, or the criteria used to determine that period;
5) 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;
6) the right to lodge a complaint with a supervisory authority;
7) where the personal data are not collected from the data subject, any available information as to their source;
8) the existence of automated decision-making, including profiling, 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.

According to Recital 63, the information provided to the data subject must be suited to allow him or her to determine if the processing is lawful. Exercising this right may be helpful in order to prepare for exercising the rights under Arts. 16–22 GDPR[123].

The ways in which the information should be provided are specified in Art. 15, para. 3. If the data subject makes the request by electronic means and does not explicitly request something else, the information shall be provided in a commonly used electronic form. Recital 63 obliges data controllers

[123] Voigt P. and von dem Bussche A., *"The EU General Data Protection Regulation (GDPR). A Practical Guide"*, Springer International Publishing AG 2017, p. 150

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

to assure that this right can be exercised "easily" and proposes one way to do so by providing remote access to a secure system which would provide the data subject with direct access to his or her personal data (if possible to establish such a system).

An example for a controller giving easy access is a health service provider using an electronic form on its website to allow data subjects to online submit access requests for personal data, which also provides paper forms in the receptions of its health clinics so that data subjects can submit requests in person[124].

The controller should also provide means for requests to be made electronically, especially where personal data are processed by electronic means. According to Recital 59, the access should be provided free of charge. For any further copies requested by the data subject, the controller may charge a reasonable fee based on administrative costs. Under Recital 63, data subjects are allowed to require access at reasonable intervals. If an individual files a request which is manifestly unfounded or excessive, in particular because of their repetitive character, the controller may either charge a reasonable fee taking into account the administrative costs of acting on the request, or refuse to act whatsoever. In any case, the controller must provide an explanation why he or she considers the request to be unfounded or excessive (Art. 12, para. 5).

The controller is obliged to respond to requests from the data subject without undue delay and at the latest within one month and to give reasons where the controller does not intend to comply with any such requests. According to the ICO Guide[125], if a data controller refuses to respond to a request, he or she must explain why to the data subject, informing them of their right to complain to the supervisory authority and to a judicial remedy in the time period stated above. The period for providing the information may be extended to three months based on the complexity and number of the requests. The controller shall inform the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay. If the controller processes a large quantity of

[124] Article 29 Working party, Guidelines on transparency under Regulation 2016/679, WP260, p. 24
[125] ICO Guide, Right of access, available at: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-of-access/

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

information concerning the data subject, Recital 63 permits him or her to ask individuals to specify the information they are requesting.

An example of such verification could be sending an access key to the requested information on an e-mail of the individual, retained in the data base of the controller.

The controller may deny access on the basis that he or she cannot verify the identity of the data subject (Art. 12, para. 2). Data controllers are obliged to apply reasonable measures in order to prevent access to data by unauthorised individuals, in particular in the context of online services and online identifiers. A controller should not retain personal data for the sole purpose of being able to react to potential requests (Recital 64). He or she should also fulfil all the general requirements under Art. 12, such as to provide information in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

The right to access should not adversely affect the rights or freedoms of others, including trade secrets or intellectual property and in particular the copyright protecting software (Art. 15, para. 4 and Recital 63). The result of the consideration of effects on others should not be a refusal to provide all information to the data subject (Recital 63). Therefore, as pointed out by the Article 29 Working party in its Guidelines on Automated individual decision-making and Profiling, controllers cannot "*rely on the protection of trade secrets as an excuse to deny access or refuse to provide information to the data subject*". To a very limited extent, controllers might conceal data that could adversely affect others when giving information to the data subject, such as blackening selected information[126].

However, it should be noted that denial of access should be possible in case where the professional secrecy must be protected. This is a matter of national legislation and the respective legal regime of the professional secrecy.

In cases where lawyer process personal data of data subjects, who are the opposite party to a dispute lawyer's professional secrecy may be a legitimate ground to deny the access to information.

[126] Voigt P. and von dem Bussche A., *"The EU General Data Protection Regulation (GDPR). A Practical Guide"*, Springer International Publishing AG 2017, p. 153,

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

8.4. Right to rectification, Art. 16

The data subject has the right to have inaccurate information rectified without undue delay. He or she could also have the right to have incomplete personal data completed, including by means of providing a supplementary statement, if it is relevant for the purposes of processing. A balancing of interests has to be carried out to determine whether a rectification is necessary and reasonable for the controller[127]. This right is a consequence of the principle of accuracy of the processed data. Data subjects carry the burden of proof for demonstrating the inaccuracy or incompleteness of personal data relating to them[128]. Under Art. 19, the controller is obliged to communicate any rectification to each recipient of personal data, unless this proves impossible or involves disproportionate effort. The controller also shall inform the data subject about those recipients if the data subject requests it. Again, all the requirements of Art. 12 should be followed.

One of the most relevant examples for legal practitioners for the exercise of this right may be rectification of the address for receiving documents by a data subject.

8.5. Right to erasure ("right to be forgotten"), Art. 17

This right to erasure or "the right to be forgotten" permits the data subject to require from the data controller to erase personal data concerning him or her without undue delay.

The data subject could exercise this right on one of the following grounds:

- the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
- the data subject withdraws consent on which the processing is based, when there is no other legal ground for the processing;
- the data subject objects to the processing;
- the personal data have been unlawfully processed;

[127] Voigt P. and von dem Bussche A., *"The EU General Data Protection Regulation (GDPR). A Practical Guide"*, Springer International Publishing AG 2017, p. 155
[128] Ibid, p. 154

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

- the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;
- the personal data have been collected in relation to the offer of information society services directly to a child.

8.5.1. Exceptions from the 'right to be forgotten'

The GDPR permits exceptions from the right of erasure in several cases. The Regulations provides for in exhaustive listing of the cases where the exceptions apply in Art. 17, para. 3:

- for exercising the right of freedom of expression and information;

Example of such expression may be an article in a newspaper, depending on the specific circumstances.

- for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

For examplem tasks related to commercial or tax law, i.e. legal practitioners shall not erase data related to payments to their employees, as they are obliged to store these data.

The notary performs tasks which are of public interest, and moreover in most of the MS it can be considered as an exercise of official authority. Therefore, the personal data they process in most of the cases cannot be erased upon the request of data subjects. Still each of the Notary's tasks should be observed ad hoc with respect to the national legislation and the obligations that it sets.

- for reasons of public interest in the area of public health; viable reasons may be preventive or occupational medicine, the assessment of the working capacity of employees, medical diagnosis, the provision of health/social care or treatment, the management of health/social care systems and services[129];

[129] Voigt P. and von dem Bussche A., *"The EU General Data Protection Regulation (GDPR). A Practical Guide"*, Springer International Publishing AG 2017, p. 160

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

National legislation may authorise employers in certain cases to process medical documents, i.e. collecting them from the data subjects, transferring them to a competent medical authority which can assess the working capacity of the employer.

- for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in so far as the right of erasure is likely to render impossible or seriously impair the achievement of the objectives of that processing;
- for the establishment, exercise or defence of legal claims; This exception refers to data that might be relevant to (future) legal claims of the controller; This is very relevant excemption for lawyers, especially when the requesting data subject is the opposite party to the one defended by the lawyer.
- also, a right to erasure should be excluded where the controller and the data subject are involved in ongoing or impending legal proceedings[130]. This is also one of the most relevant exemptions concerning legal practitioners.

Pursuant to Art. 17, para. 2, where the controller has made the personal data public and is obliged to erase the personal data, he or she, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure.

An example of such situation may be when a search engine is obliged to erase data and it should inform sites containing the same personal data.

It should be noted that under Art. 19 a controller has the obligation to inform any recipient of data for the erasure, unless this proves impossible or involves disproportionate effort. As the right to erasure is a subjective right, the data subject has to prove its existence. The data subjects should be obliged to specify the grounds on which they wish to exercise the right and should also prove additional circumstances[131]. When it comes to the exceptions, the controller carries the risk for

[130] Ibid;
[131] Voigt P. and von dem Bussche A., *"The EU General Data Protection Regulation (GDPR). A Practical Guide"*, Springer International Publishing AG 2017, p. 159

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

the existence of an exception from the right of erasure[132].

8.6. Right to restriction of processing, Art. 18

The right to restriction means that data subjects can limit the way that an organisation uses their data[133]. This is not an absolute right, it could be exercised only under certain circumstances, enumerated in Art. 18, para. 1:

1) when the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data, or in other words, the restriction on these grounds is temporary.
2) when the processing is unlawful, and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;
3) when the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims;

These grounds relate to the general obligation of the controller to erase data that is no longer needed for the purposes of processing.

4) when processing is based on the legitimate grounds in Art. 6, para. 1, lit. e - for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, or in lit. f - for the purposes of the legitimate interests pursued by the controller or by a third party, and the data subject has objected; in this case the processing should be restricted until it is verified whether the legitimate grounds of the controller override those of the data subject. In this case the restriction is also temporary.

Storing of personal data is outside the scope of Art. 18 and cannot be restricted, as the restricted information should be available and therefore cannot be erased. In some cases, processing can be permitted even when one of the conditions in Art. 18, para. 1 is present. Such cases are:

1) with the data subject's consent;

[132] Ibid, p. 161
[133] ICO Guide, Right of restriction, https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-restrict-processing/

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

2) for the establishment, exercise or defence of legal claims;
3) for the protection of the rights of another natural or legal person;
4) for reasons of important public interest of the Union or of a Member State.

These are the only conditions under which the restriction could be lifted. If that happens, the data subject must be informed before the lifting (Art. 18, para. 3). The controller could refuse to restrict the processing under the general provision of Art. 12, para. 5.

The GDPR suggests methods for restricting the processing. Such could be temporarily moving the selected data to another processing system, making the selected personal data unavailable to users, or temporarily removing published data from a website. In automated filing systems, the restriction of processing should in principle be ensured by technical means so that the personal data are not subject to further processing operations and cannot be changed. In such a case, the GDPR stipulates that the fact that the processing of personal data is restricted should be clearly indicated in the system (Recital 67).

When dealing with requests for restriction of processing, data controllers should have in mind Art. 19 of the GPDR, which imposes an obligation to communicate the restriction to the recipients of personal data, unless this proves impossible or involves disproportionate effort. Also, controllers have to comply with the general provisions of Art. 12. The GDPR does not specify how to make a valid request. Therefore, according to the ICO, an individual can make a request for restriction verbally or in writing[134].

According to the ICO guide, it is better for data controllers to automatically restrict the processing whilst they are considering the accuracy of the data or the legitimate grounds for processing[135].

8.7. Right to data portability, Art. 20

This right allows for data subjects to receive the personal data that they have provided to a data controller, in a structured, commonly used and machine-readable format, and to transmit those data

[134] ICO Guide, Right of restriction, https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-restrict-processing/
[135] Ibid

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

to another data controller without hindrance. First, in order to fall under the scope of data portability, processing operations must be based on the data subject's consent (either pursuant to Art.6, para. 1, lit. a or pursuant to Art. 9, para. 2, lit. a, when it comes to special categories of personal data) or on a contract to which the data subject is a party. Second, the processing must be carried out by automatic means.

Possible data for which this right may be used can be records of purchases in online commerce sites which contain personal data. In the mentioned case the data will be processed on the basis of the performance of a contract to which the data subject is a party. Another illustrative example is the one with the cloud service provider. A client can request that all data need to be transferred to a new service provider.

"Hindrance" under Art. 20 can be characterised as any legal, technical or financial obstacle placed by data controllers in order to refrain or slow down access, transmission or reuse by the data subject or by another data controller. Such hindrance could be: fees asked for delivering data, lack of interoperability, excessive delay or complexity to retrieve the full dataset[136].

The right of data portability comprises a few elements:

1) A right to receive personal data – to receive a subset of the personal data processed by a data controller concerning him or her, and to store those data for further personal use: the difference between this right and the right to access lies in the fact that the first one offers an easy way for data subjects to manage and reuse personal data themselves[137].
2) A right to transmit personal data from one data controller to another data controller - the ability of data subjects to transmit the data they have provided to another service provider.

For example, in case a consumer would like to conclude a new contract with a telecom operator, he/ she might request the transmission of data provided to the former telecom to the new one.

3) Controllership - data portability guarantees the right to receive personal data and to process them according to the data subject's wishes.

[136] Article 29 Data Protection Working Party, Guidelines on the right to data portability, WP 242 rev.01, p.15
[137] Article 29 Data Protection Working Party, Guidelines on the right to data portability, WP 242 rev.01, p.4

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

The GDPR stipulates that the exercise of the right to data portability shall be without prejudice to the right to erasure. In other words, if a data subject requests transfer of their data, that does not automatically mean that they are renouncing the service and that they also want to exercise their right of erasure.

Data, created by the controller on the basis of the data "provided by the subject" (inferred data or derived data), are not considered to be provided by the subject.

For example, the profile created in the context of risk management and financial regulations cannot be considered "provided by the subject".

The only accepted and retained data should be those which are necessary and relevant to the provided by the receiving data controller service. Receiving data controllers are not obliged to accept and process personal data transmitted after a data portability request[138].

Art. 20, para. 2 imposes obligations on data controllers for transmitting the portable data directly to other data controllers "when technically feasible". According to Recital 68, data controllers should be encouraged to develop interoperable formats that enable data portability. However, they do not have an obligation to adopt or maintain processing systems which are technically compatible.

Article 20, para. 4 states that compliance with this right shall not adversely affect the rights and freedoms of others. This could happen if the transmission of data from one data controller to another would prevent third parties from exercising their rights as data subjects under the GDPR. Where personal data of third parties are included in the data set required by the data subject, another legal basis for the processing must be established[139] (for example legitimate interest).

When fulfilling their obligations under Art. 20, data controllers should have in mind the general provisions of Art. 12. 8.8. Right to object, Art. 21

The data subject can object at any time, on grounds relating to his or her particular situation, to processing of personal data concerning him or her, when it is based either on performance of a task

[138] Article 29 Data Protection Working Party, Guidelines on the right to data portability, WP 242 rev.01, p. 6
[139] Ibid. p. 11

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

carried out in the public interest or in the exercise of official authority vested in the controller (Art. 6, para. 1, lit. e) or on the legitimate interests pursued by the controller or by a third party (Art. 6, para. 1, lit. f), including profiling based on those provisions. Art. 21 is directed against lawful processing activities that do not correspond to the will of the data subject, because of new circumstances that influence the initial balancing of interests.[140]. "Particular situation" may refer to the data subject's family circumstances or a professional interest in confidentiality[141]. The right to object is not a new conception in data protection acts, but the GDPR introduces some changes. The Regulation reverses the burden and requires controllers to demonstrate that they either have compelling grounds for continuing the processing, or that the processing is necessary for the establishment, exercise or defence of legal claims. The compelling grounds of the controller should also override the interests, rights and freedoms of the data subject. If controllers cannot demonstrate that the relevant processing activity falls within one of these two grounds, they must cease that processing activity. This could be especially problematic for organisations that rely on their own legitimate interests as a lawful basis for processing personal data[142]. Exercising the right to object will often require an evaluation of the interests of data subjects against the interests of data controllers or third parties. How exactly should this evaluation be performed is unclear, because of some contradictions between the general grounds for processing in Art. 6 (which requires the rights and freedoms of the data subjects to be fundamental), Art. 21, para. 1 and Recital 69 (which also mentions "fundamental" rights and freedoms)[143]

The GDPR does not permit exceptions from the right to object when it comes to direct marketing purposes. Profiling to the extent that it is related to such direct marketing is also included.

---

[140] Voigt P. and von dem Bussche A., *"The EU General Data Protection Regulation (GDPR). A Practical Guide"*, Springer International Publishing AG 2017, p. 177

[141] Ibid

[142] Gabel, Detlev, Dr., Hickman, Tim, Chapter 9: Rights of data subjects – Unlocking the EU General Data Protection Regulation, 3 September 2017, available at: https://www.whitecase.com/publications/article/chapter-9-rights-data-subjects-unlocking-eu-general-data-protection-regulation

[143] For additional elaboration on the evaluation of balance of interests in Art. 21 see Ausloos, Jef, Balancing in the GDPR: legitimate interests v. right to object, 28 February 2017, available at: https://www.law.kuleuven.be/citip/blog/balancing-in-the-gdpr-legitimate-interests-v-right-to-object/

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

An example for such activity could be profiling of a user of online commerce platform based on their previous purchases, in order to send to them information about relevant products.

In this case the Regulation does not require the data subject to have grounds for objection – the condition in Art. 21, para. 1 that the subjects must give grounds relating to their particular situation is not present.

The right to object has some similarities with the right to erasure. The key difference between the two conceptions is that the former focuses on a specific processing operation, whereas the latter relates to the personal data itself. This distinction is crucial in modern-day context, because the same personal data is often processed for an incalculable number of purposes. The right to object only prevents further processing for one or more separate purposes, whereas the right to erasur prevents processing of any kind as the data can no longer be stored by the controller[144].

Controllers are obliged to inform data subjects of their rights to object to processing. This obligation derives from the provision of Art. 13, para. 2, lit. b, but also from the explicit provision of Art. 21, para. 4. The latter stipulates that at the latest at the time of the first communication with the data subject, the right to object shall be explicitly brought to the attention of the data subject. It must be presented clearly and separately from any other information.

In the context of the use of information society services, and notwithstanding the Directive on privacy and electronic communications, the data subject may exercise his or her right to object by automated means using technical specifications (e.g. tools to block the tracking of one's web browsing behaviour[145]).

Where personal data are processed for scientific or historical research purposes or statistical purposes, the data subjects can object if they can prove grounds relating to their particular situations and if the processing is not necessary for the performance of a task carried out for reasons of public interest. The necessity of processing for public purposes should be proven by the controllers. In other words,

[144] Ausloos, Jef, The Interaction between the Rights to Object and to Erasure in the GDPR, 25 August 2016, https://www.law.kuleuven.be/citip/blog/gdpr-update-the-interaction-between-the-right-to-object-and-the-right-to-erasure/

[145] Ibid

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

the data subjects can object to such processing only when it is based on the exercise of official authority vested in the controller or on the controller's or a third party's legitimate interest. (See Art. 89 for this specific kind of processing).

A successful objection gives rise to the data subject's right to erasure.

- This right could be exercised against legal practitioners mostly in the hypothesis where data subjects which are not clients, require their data not to be processed. In the majority of cases the legal practitioners could rely on one of the two exemptions to this right.

8.9. Automated individual decision making including profiling, Art. 22

Article 22 of GDPR has been thoroughly examined in the Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679. In order to understand the rights and obligations under this Article, first of all an analysis of automated decision making and profiling should take place.

Not every automated decision making involves profiling. Automated decision-making may partially overlap with or result from profiling[146]. Profiling will be in place in each case, where personal data has been processed automatically in order to evaluate personal aspects, in particular to evaluate or make predictions about individuals – their *performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements*[147]. The evaluation purpose is the key notion to be considered when defining whether a processing involves profiling – therefore a mere classification based on different personal aspects should not be considered profiling when the purposes is not to evaluate these aspects.[148]

[146] Art. 29 Data Protection Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, WP 251
[147] Recital 71, GDPR.
[148] Art. 29 Data Protection Working Party, Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679, WP 251

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

It should be stressed that neither profiling, nor automated decision making is prohibited under GDPR. On the contrary, both GDPR and Article 29 Working Party acknowledge the benefits of these instruments and their significance for both public and private sector[149]. What GDPR restricts is decision-making based *solely* on automated processing, *including profiling*, which produces *legal effects* concerning him or her *or similarly significantly* affects him or her.

Thus, the first element of this provisions is the term "solely". As Article 29 Working party clarifies, one should be very mindful when analysing whether a decision is based "solely" on automated processing, which means that no human involvement is in place. Article 29 Working Party has specifically stated that controllers cannot avoid the application of Article 22 by "*fabricating human involvement*"[150].

The other two elements that need to be addressed is the requirement for "legal" or "similarly significant effect". Where the legal effect in most of the cases can be easily identified, defining the similarly significant effect is the challenge of this provision. Article 29 Working Party acknowledges that this could be a difficult task. It sets the following criteria for deciding the significance of the impact:

- significantly affect the circumstances, behaviour or choices of the individuals concerned;
- have a prolonged or permanent impact on the data subject; or
- at its most extreme, lead to the exclusion or discrimination of individuals.[151]

As Article 22, para. 1 sets a general prohibition for taking solely automated decisions, including profiling, paragraph 2 envisages several exceptions, where such processing can be undertaken:

- necessary for the performance of or entering into a contract. In order to apply this exception, the controller should be able to demonstrate that this "*type of processing is necessary, taking into*

[149] For instance, law enforcement authorities in some countries may impose administrative fines on the base of automated decision processing when using data from speed detecting cameras.
[150] Art. 29 Data Protection Working Party explains that *to qualify as human involvement, the controller must ensure that any oversight of the decision is meaningful, rather than just a token gesture. It should be carried out by someone who has the authority and competence to change the decision.*
[151] Ibid.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

account whether a less privacy-intrusive method could be adopted"[152]

- authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or
- based on the data subject's explicit consent.[153]

Chapter 9: Legal position of the data processor

Data processor is defined in the GDPR as a natural or legal person, public authority, agency or other body that processes personal data on behalf of the controller - Art. 4 No. 8 GDPR. The existence of a processor depends on a decision taken by the controller, who can either process data within its organisation (e.g., through its own employees) or delegate all or part of the processing activities to an external organisation, rendering the latter a 'processor'[154]. The relations between the controller and processor should be governed by a written contract, which contains certain statutory mandated clauses.

9.1. Indirect obligations, Art. 28, 29

As opposed to the processors' direct obligations, which derive from Art. 30, para. 2 and 32, and are aimed at the data processor, the GDPR also imposes indirect obligations which derive from the requirement the data processor to follow the controller's instructions and to have a written contract with him or her. The GDPR introduces certain obligatory clauses that must be present in the contract and, as they bind the processor, they turn into obligations for every processor acting under EU law.

[152] Ibid.
[153] See section 6.1.1 of this document.
[154] Voigt P. and von dem Bussche A., "The EU General Data Protection Regulation (GDPR). A Practical Guide", Springer International Publishing AG 2017, p. 28

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

9.1.1 Compliance with the controller's instructions, Art. 29

The GDPR imposes requirements for the contract or other legal act under Union of Member State law between the processor and the controller. Art. 28, para. 3 stipulates that the act shall contain a clause about the instructions from the controller, including with regard to transfers of personal data to a third country or an international organisation. The data processor has an obligation to process the data only on documented instructions from the controller or when required to do so by Union or Member State law to which the processor is subject. In the latter case, the processor shall inform the controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest. The requirement for documenting the instructions is meant to facilitate the process of proving compliance with the GDPR and is an obligation of the processor, not of the controller[155]. If a processor acts outside or against the instructions of the controller, he / she may be liable to pay damages in legal proceedings or be subject to fines or other penalties or corrective measures.

9.1.2 Conflicts between controller instructions and applicable law, Art. 28, para. 3

According to Art. 28, para. 3 lit. h the contract between the controller and the processor shall contain an obligation for the processor to make available to the controller all information necessary to demonstrate compliance with the obligations laid down in Art. 28 and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller. The next subparagraph states that with regard to lit. h), the processor shall immediately inform the controller if, in its opinion, an instruction infringes GDPR or other Union or Member State data protection provisions.

For example, such an instruction would be to process special categories of personal data under Art. 9, para. 1, without any of the prerequisites to do so.

[155] Voigt P. and von dem Bussche A., "*The EU General Data Protection Regulation (GDPR). A Practical Guide*", Springer International Publishing AG 2017, p. 81-82

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

In practice, the processor may refuse to execute the instructions based on subjective legal assessment that is supposed to protect it from an obligation to act upon instructions that contradict its legal conviction. It is not specified by law how the controller shall react and how disagreements about instructions shall be resolved[156]. There is no obligation for the processor to conduct a legal assessment of the controller's instructions.

9.1.3 Obligation of confidentiality, Art. 28, para. 3 lit. b, Art. 29

The contract between the controller and the processor must ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality. Any person with access to personal data acting under the authority of a controller or a processor shall process such data only on instructions from the controller or processor. Such person could be any employee of a data controller, or a section or unit within a company which is processing personal data for the company as a whole. Someone who is not employed by the data controller but is contracted to provide a particular data processing service (such as a tax adviser or accountant) is a data processor and has the corresponding obligations under the GDPR. If the person acts on requirement of Union or Member State law, he or she may not follow the instructions of the controller or processor.

An example of processors whose activities are often regulated by statutory law are accounting and taxation. When an entity outsources these operations to an external accounting firm, the latter acts as a processor. They act only upon instructions from the controllers (their clients) but are often subject to additional obligations under specific national legislation.

9.1.4 Appointment of sub-processors, Art. 28, para. 2 and 4

Sub-processors are appointed only with the explicit written authorisation of the controller. This authorization could be specific or general. In the second case the processor shall inform the controller of any intended changes concerning the addition or replacement of other processors, giving the

[156] Voigt P. and von dem Bussche A., "*The EU General Data Protection Regulation (GDPR). A Practical Guide*", Springer International Publishing AG 2017, p. 83

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

controller the opportunity to object to such changes. Para. 4 stipulates that where a processor engages another processor for carrying out specific processing activities on behalf of the controller, the same data protection obligations as set out in the contract or other legal act between the controller and the processor shall be imposed on that other processor by way of a contract or other legal act under Union or Member State law. In other words, the contract between a processor and a sub-processor must at least contain the same data protection obligations as set out in the contract between the processor and the controller. This second contract between the processor and sub-processor shall provide sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of the GDPR. If the other processor fails to fulfil its data protection obligations, the initial processor shall remain fully liable to the controller for the performance of the other processor's obligations. A subcontractor should not be considered a sub-processor of personal data, i.e. 'another processor', unless he/ she actually has access to personal data and intends to access personal data[157].

9.1.5 Effect of infringement, Art. 28, para. 10

Para. 10 states that without prejudice to Articles 82, 83 and 84, if a processor infringes the GDPR by determining the purposes and means of processing, it shall be considered to be a controller in respect of that processing. The emphasis is on which entity determines the purposes and means of processing in reality in order for it to bear the respective obligations and responsibilities as a controller. However, this entity needs to have a legitimate ground for processing the personal data as a controller.

[157] According to Hon, W Kuan, Dr., Data Protection: Controllers, Processors, Contracts, Liability – the ICO Draft Guidance, 06 October 2017, available at: https://www.scl.org/articles/10017-data-protection-controllers-processors-contracts-liability-the-ico-draft-guidance

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

9.2. Direct obligations

9.2.1. Accountability, Art. 30, para. 2

Each processor and, where applicable, the processor's representative shall maintain a record of all categories of processing activities carried out on behalf of a controller. This record must contain:

- the name and contact details of the processor or processors and of each controller on behalf of which the processor is acting, and, where applicable, of the controller's or the processor's representative, and the data protection officer;
- the categories of processing carried out on behalf of each controller; this requirement refers to the types of data processing for example on basis of process/steps performed (batch, real-time, online, multi and time-sharing processing).
- transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1) (in the absence of an adequacy decision pursuant to Article 45(3), or of appropriate safeguards pursuant to Article 46, including binding corporate rules), the documentation of suitable safeguards; the recipients do not have to be individually identified[158].
- where possible, a general description of the technical and organisational security measures referred to in Article 32(1).

The record must be written and must be made available to the supervisory authority on request. This obligation does not apply to an enterprise or an organisation employing fewer than 250 persons. There are three exceptions from this rule:

- if the processing carried out is likely to result in a risk to the rights and freedoms of data subjects; as every data processing poses a risk to the rights and freedoms of subjects, the

[158] Van Canneyt, Tim, Provoost, Soo Mee, Belgian DPA publishes recommendation on GDPR record keeping obligation, 4 July, 2017, available at: http://privacylawblog.fieldfisher.com/2017/belgian-dpa-publishes-recommendation-on-gdpr-record-keeping-obligation/

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

presumable idea of this exception is to include only processing which does not pose a minor risk[159] .

An example for such activity that is occasional, but poses a risk, is profiling of customers for the purposes of insurance-risk classification done by a small insurance company, because this kind of activity is considered intrusive[160].

- if the processing is not occasional; data processing is 'occasional' if the processing in question only plays a subordinate role in the activity of the processor and only occurs for a very short time period or once[161];

Example for such activity could be an internal staff engagement survey that the company performs once a year.

- if the processing includes special categories of data as referred to in Article 9, para. 1 or personal data relating to criminal convictions and offences referred to in Article 10.

Records are an important accountability instrument, they help data processors to comply with the GDPR. The regulation does not require the records to be public, they are considered internal documents[162]. The records must contain detailed information on all processing activities, regardless of how long they have been carried out. According to the Belgian Privacy Commission, Art. 30 should be read in conjunction with the requirement to identify the purpose of the processing and one record should correspond to one purpose of the processing, even if the processing activities aimed at that purpose are more than one[163]. Additionally, the obligation to keep records should be understood as a

[159] Voigt P. and von dem Bussche A., *"The EU General Data Protection Regulation (GDPR). A Practical Guide"*, Springer International Publishing AG 2017, p. 46
[160] ICO Guide, Do all organisations need to document their processing activities?, available at: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/documentation/who-needs-to-document-their-processing-activities/
[161] Voigt P. and von dem Bussche A., *"The EU General Data Protection Regulation (GDPR). A Practical Guide"*, Springer International Publishing AG 2017, p. 54
[162] According to Van Canneyt, Tim, Provoost, Soo Mee, in Belgian DPA publishes recommendation on GDPR record keeping obligation, 4 July, 2017, available at: http://privacylawblog.fieldfisher.com/2017/belgian-dpa-publishes-recommendation-on-gdpr-record-keeping-obligation/
[163] Ibid

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

dynamic obligation[164]: the processors must re-assess the accuracy of the records on a regular basis in accordance with the principles of the GDPR (Art. 5, para. 1, lit. d).

- Legal practitioners may maintain records of the data processed about their employees, or clients.

9.2.2. Data Security, Art. 32, para. 1

The protection of personal data is guaranteed by the obligation of controllers and processors to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk. The obligation of the processor includes ensuring that any individual acting under its authority shall only process personal data according to the instructions of the controller or under Union of State law (Art. 32, para. 4 GDPR). Without being exhaustive, the GDPR enumerates the minimal measures that must be taken:

- the pseudonymisation and encryption of personal data - the data is altered by cryptographic operation. Encrypted data can still be attributed to a specific data subject, but in order to do so additional information – a key of decryption – is needed. The additional information allowing identification must be kept separately.
- the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; in other words, all data should be available to users, and measures should be taken to ensure that it is not read or tampered with by unauthorized persons, whether accidentally or on purpose.
- the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident - among other things, entities should be able to establish immediately whether a data breach occurred and communicate it. The recovery of the data should happen as quickly as possible.
- a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing - the GDPR requires

[164] Ibid

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

maintenance of the measures taken and proportionality between the frequency of testing, assessing and evaluating the effectiveness and the level of risk for data security[165].

It should be stressed that the controller needs to make an assessment of the appropriate measures – the listed measures are not mandatory and may appear to be disproportionate to the respective processing operation.

The GDPR introduces a risk-based approach, according to which the factors considered when choosing the appropriate security measures should be:

- the state of the art.
- the costs of implementation and the nature, scope, context and purposes of processing – the GDPR introduces a proportionality principle, which concerns the controllers and processors. The costs of implementation should be proportionate to the category of processing and to the risk for the rights and freedoms of data subjects.
- the risk and severity for the rights and freedoms of natural persons.

Recital 75 determines that there is a risk for the rights and freedoms of data subjects when physical, material or non-material damage could be caused by the data processing. Such damage could occur in particular where:

- the processing may give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy;
- there is unauthorised reversal of pseudonymisation, or any other significant economic or social disadvantage;
- data subjects might be deprived of their rights and freedoms or prevented from exercising control over their personal data;
- personal data categorized as special under Art.9 is processed (data revealing racial or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, genetic data, data concerning health or data concerning sex life or criminal convictions and offences

[165] Voigt P. and von dem Bussche A., *"The EU General Data Protection Regulation (GDPR). A Practical Guide"*, Springer International Publishing AG 2017, p. 40

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

or related security measures);

- personal aspects are evaluated, in particular analysing or predicting aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, in order to create or use personal profiles;
- processing personal data of vulnerable persons, in particular of children;
- processing involves a large amount of personal data and affects a large number of data subjects.

Recital 76 introduces the notion of objective assessment, which must establish whether data processing operations involve a risk or a high risk. The GDPR does not provide a definition of "high risk", but rather implies that all risks can become "high risk", depending on their "likelihood and severity" as determined in a risk assessment process by reference to the nature, scope, context and purpose of processing. Additionally, Art. 32, para. 2 stipulates that in assessing the appropriate level of security, account must be taken in particular of the risks that are presented by personal data breach (a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed). Processors must adjust their security measures to match the probability and severity of a breach against the potential impacts on rights and freedoms of data subjects.

As already mentioned in chapter 7, legal practitioners are generally data controllers and should be careful of the processors they may contract because of the specificity of the data they process (for instance, the cloud or mail service provider they use).

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

Key concepts:

Indirect obligations: processors have obligations deriving from their written contract with the controller, because of the list of obligatory clauses which must be included in it under the GDPR. The most important consequence from this provision is that a processor who does not follow the lawful instructions of the controller is liable under Art. 82 for the damage caused to data subjects by processing.

Direct obligations of the processor: to maintain a record of all categories of processing activities carried out on behalf of a controller and to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

Situations when processors should be considered controllers: if a processor infringes the GDPR by determining the purposes and means of processing, it shall be considered a controller in respect of that processing.

Most important notions for legal practitioners: legal practitioners should keep in mind the direct liability of data processors under the GDPR and the requirements for the contracts between controllers and processors and processors and sub-processors.

Chapter 10: Sanctions and liability

10.1. Remedies available to data subjects

The GDPR provides data subjects with both judicial and extra-judicial remedies, allowing them to defend their rights under the regulation.

10.1.1. Right to lodge a complaint with a supervisory authority, Art. 77

Every data subject has the right to lodge a complaint with a supervisory authority in the Member State of its habitual residence, place of work or place of the alleged infringement if it considers that the processing of its personal data infringes the GDPR. This remedy must be available notwithstanding any other administrative or judicial remedies. The supervisory authority has the obligation to inform

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

the complainant on the progress and the outcome of the proceedings including the possibility of a judicial remedy. It is important to note that the DPA to which the complaint is addressed will not necessarily be the DPA that is responsible for regulating the relevant controller[166][167].

An individual is able to make complaints to the DPA in their Member State, at which point that regulator shall engage in a co-operation procedure with other "concerned" supervisory authorities, as outlined in Art 57, para 1, lit g and h, GDPR.

10.1.2. Right to an effective judicial remedy against a supervisory authority, Art. 78, para. 1 and 2

Each data subject shall have the right to an effective judicial remedy against the DPA. This right is established specifically for data subjects and concerns namely two infringements of the GDPR by the DPA: 1) incompliance with the requirement to handle the complaint or 2) incompliance with the requirement to inform the data subject within three months on the progress or outcome of the complaint. This right must exist without prejudice to any other administrative or non-judicial remedy.

In addition to the right of the data subjects under para. 2, under para. 1 every natural or legal person shall have the right to an effective judicial remedy against a DPA, if its decision is binding and concerns that person. In other words, a complainant before a court must be directly affected by the DPA's decision. This right is also without prejudice to any other administrative or non-judicial remedy. Proceedings against a DPA shall be brought before the courts of the Member State where it is established.

---

[166] Gabel, Detlev, Dr., Hickman, Tim, Remedies and sanctions – Unlocking the EU General Data Protection Regulation, 22 July 2016, available at: https://www.whitecase.com/publications/article/chapter-16-remedies-and-sanctions-unlocking-eu-general-data-protection

[167] The DPA jurisdiction for supervising data controllers and processors is determined under Article 56 **Competence of the lead supervisory authority.** Where the controller or processor is established in several Member States, the supervisory authority of the main establishment shall be competent as "lead authority" (the "one-stop shop"). The main establishment of a controller should be the place of its central administration in the Union, unless the decisions on the purposes and means of the processing of personal data are taken in another establishment of the controller in the Union.[167] The main establishment of the processor should be the place of its central administration in the Union or, if it has no central administration in the Union, the place where the main processing activities take place in the Union. In cases involving both the controller and the processor, the competent lead supervisory authority is the supervisory authority of the Member State where the controller has its main establishment. The local DPA will remain competent to handle a matter if it relates only to a local establishment or affects data subjects only in its Member State (except for data transfers).

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

10.1.3. Right to an effective judicial remedy against a controller or processor, Art. 79

Each data subject has the right to an effective judicial remedy if he or she considers that his or her rights under the GDPR have been infringed as a result of the processing of his or her personal data in non-compliance with the regulation. This right exists without prejudice to any available administrative or non-judicial remedy, including the right to lodge a complaint with a supervisory authority, discussed above. Art. 79, para. 2 establishes the competence of courts in such matters - proceedings against a controller or a processor shall be brought before the courts of the Member State where the controller or processor has an establishment[168]. Alternatively, such proceedings may be brought before the courts of the Member State where the data subject has his or her habitual residence, unless the controller or processor is a public authority of a Member State acting in the exercise of its public powers. So where, the controller/processor has no establishment in EU (having in mind the territorial scope of the Regulation), data subjects can file a complaint in accordance to the alternative prorogation of jurisdiction. The damage suffered by the date subject could be both material or non-material and no definition of non-material damage is provided[169]. Construing Art. 79 , para 1, it could be concluded that there is no obligation to the claimant to prove damage, simply that his or her rights under the Regulation have been are infringed[170]. The right to a judicial remedy against the controller or processor is limited to those cases where the specific rights of data subjects have been infringed as opposed to the right to complain to the supervisory authority which applies in any cases where the data subject considers that he/she is affected by a non-compliance with the Regulation[171].

10.1.4. Right to representation by not-for-profit body, organisation or association, Art. 80

The data subject has the right to mandate a not-for-profit body, organisation or association to lodge a complaint on his or her behalf with a DPA and before a court against a DPA or to file a claim against

[168] See footnote number 164.
[169] O'Riordan, John, Bredin, Peter, GDPR: Judicial Remedies, July 2017, available at: http://www.dilloneustace.com/download/1/Publications/Regulatory%20and%20Compliance/GDPR-Judicial%20Remedies%2020170726.pdf,
[170] Ibid.
[171] Bolgar, Peter, Kelly, Jeanne, Enforcement and Remedies under the GDPR, 18 September 2017, available at: https://www.lexology.com/library/detail.aspx?g=35f640a4-0a8a-4a81-becb-392fcb201042

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

a controller or processor, as well as to exercise the right to receive compensation (where provided for by Member State law). The GDPR requires the bodies, organisations or associations to be properly constituted in accordance with the law of a Member State, to have statutory objectives which are in the public interest, and to be active in the field of the protection of data subjects' rights and freedoms with regard to the protection of their personal data. The notion is to increase the involvement of consumer protection associations, which could build up pressure on controllers/processors to reach compliance with the GDPR[172]. Additionally, Para. 2 of Art. 80 states that Member States may allow such bodies, organisations or associations to lodge complaints with the DPA or before a court (both in the same Member State as the entity) independently of a data subject's mandate, if it considers that the rights of a data subject under the GDPR have been infringed as a result of the processing.

10.1.5. Right to compensation and liability, Art. 82, para. 1

Any person who has suffered material or non-material damage as a result of an infringement of the GDPR shall have the right to receive compensation from the controller or processor for the damage suffered. According to Recital 146, the notion infringement is to be interpreted in a broad manner and, thus, includes processing that violates delegated and implementing acts adopted in accordance with the GDPR, as well as EU Member State law specifying rules of the GDPR. Individuals should receive full and effective compensation for the damage they suffered, and the concept of damage should be broadly interpreted in the light of the case-law of the European Court of Justice. 'Any person' suffering damage might claim compensation. The right to compensation shall, first entitle the data subject to compensation. However, it could also entitle other individuals who suffered a damage, if there is sufficient causal link between the third party's damage and the infringement of data protection law[173]. This claim is without prejudice to any claims for damage deriving from the violation of other rules in Union or Member State law.

According to Art. 82, any controller involved in processing shall be liable for the damage caused by processing which infringes the GDPR. A processor shall be liable for the damage caused by processing

[172] Voigt P. and von dem Bussche A., *"The EU General Data Protection Regulation (GDPR). A Practical Guide"*, Springer International Publishing AG 2017, p. 216
[173] Ibid, p. 206

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

only where it has not complied with obligations of the GDPR specifically directed to processors or where it has acted outside or contrary to lawful instructions of the controller. The claimant bears the burden of proof in relation to the controller's and processor's liability. As the claimant does not have detailed insight into the controller's/processor's operations, in order to establish the controller's/processor's liability, a plausible claim satisfies the claimant's burden of proof[174]. The competent courts are those of the Member State where the controller or processor has an establishment or the courts of the Member State where the data subject has his or her habitual residence, unless the controller or processor is a public authority acting in the exercise of its public powers. Each controller or processor is jointly and severally liable for the entire damage in order to ensure effective compensation of the data subject. In other words, the data subject can claim the entire damage from every controller or processor.

10.2. Liability of data controllers and data processors

The liability of the controller has a larger scope in comparison with the liability born by the processor, as any controller involved in processing is liable for all damages caused by processing which infringes the GDPR. The controller is obliged to implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with the GDPR. As stated above, data controllers are liable:

1) under Art.79 for any non-compliance with the GDPR;

2) under Art. 82 for any material or non-material damage as a result of an infringement of the GDPR while processing data, including for actions of the processor, if it acted contrary to the GDPR or to the instructions of the controller.

The burden of proof is on the controller as to its responsibility for the event giving rise to the damage. If it manages to prove non-responsibility, the controller is exempt from liability. Each controller or processor is held liable for the entire damage and can claim back that part of the compensation corresponding to the other controller or processor's part of responsibility for the damage. The GDPR

[174] Voigt P. and von dem Bussche A., *"The EU General Data Protection Regulation (GDPR). A Practical Guide"*, Springer International Publishing AG 2017, p. 207

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

contains no exemption for force majeure cases in contrast with Art. 23, para 2 of the Data Protection Directive. Therefore, controllers may still bear the risk in such situations in case they fail to prove that all necessary technical and organisational measures have been taken[175].

The novelty in the GDPR is that the processor can be directly held liable for violations of its obligations under the Regulation. The processor bears liability in two cases: when its actions are not compliant with its obligations under the GDPR, or when it did not follow lawful instructions of the data controller.

10.3. Administrative fines and other penalties, Art. 83 and 84

Administrative fines are imposed by the supervisory authority and according to Art. 83, para. 1 they must be effective, proportionate and dissuasive. There are several factors that have to be taken into account by supervisory authorities when deciding the level of fine. They are enlisted in para. 2, lit. a – k:

- the nature, gravity and duration of the infringement taking into account the nature scope or purpose of the processing concerned as well as the number of data subjects affected, and the level of damage suffered by them;
- the intentional or negligent character of the infringement; the definitions of "intention" and "negligence" under the GDPR follow the well-established notions in EU law.

  The Article 29 Data Protections Working Party gives an example for intentional infringement with the trade of personal data for marketing purpose i. e. selling data as 'opted in' without checking/disregarding data subjects' views about how their data should be used[176].

  It regards infringements caused by circumstances such as human error, failure to check for personal data in information published, failure to apply technical updates in a timely manner and others as indicative of negligence.

[175] Detlev, Gabel, Dr. Hickman, Tim, Chapter 16: Remedies and sanctions – Unlocking the EU General Data Protection Regulation, 22 July 2016, available at: https://www.whitecase.com/publications/article/chapter-16-remedies-and-sanctions-unlocking-eu-general-data-protection

[176] Article 29 data protection working party, Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679, WP 253, p. 12

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

- any action taken by the controller or processor to mitigate the damage suffered by data subjects;
- the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them; to what extent the controller "did what it could be expected to do" given the nature, the purposes or the size of the processing in light of the obligations under the GDPR. Best practices and industry standards are to be taken into consideration when applying this criterion.
- any relevant previous infringements by the controller or processor;
- the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement;[177].
- the categories of personal data affected by the infringement;
- the manner in which the infringement became known to the supervisory authority, in particular whether, and if so to what extent, the controller or processor notified the infringement; it should be noted that if controller merely fulfilled the statutory imposed obligation for notification of the DPA, this cannot be interpreted as an attenuating/ mitigating factor;
- compliance with previously-ordered measures concerning the sate subject matter;
- adherence to approved codes of conduct or approved certification mechanisms;
- any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement.

The proactive conduct of data controllers and processors and their policy of communicating breaches may result in a smaller fine. For example, a controller or a processor may take timely action to stop the infringement from continuing or expanding to a level or phase which would have had a far more serious impact[178].

If the data subjects have suffered damage, the level of the damage has to be taken into consideration[179].

[177] Article 29 data protection working party, Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679, WP 253, p. 15
[178] Ibid, p. 13
[179] Ibid, p. 7

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

It is important for data controllers and data processors to review the factors and establish what steps can be taken to limit the level of any possible fine[180]. Also, it should be noted that in terms of the amount of a fine, it will depend on which Article of the GDPR has been breached as the GDPR provides for two categories of fines[181]: the first category is for infringements listed in Art. 83, para. 4 which is up to 10 000 000 EUR, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher. This fine is imposed for infringements like failure to fulfil the notification obligation, failure to designate a DPO, failure to implement appropriate technical and organisational measures and others. The second category is under Art. 83, para. 5, which imposes higher fines. The maximum fine under is 20,000,000 EUR or, where the breaching party is an undertaking, up to 4% of the total worldwide annual turnover in the preceding year. The infringements of this category are considered graver and include, inter alia, processing personal data in a manner which is not lawful, fair and transparent, failure to prove consent of the data subject, collecting personal data for a purpose which is not specified, explicit and legitimate. According to Recital 150, the definition of an undertaking under the GDPR coincides with the one applied to competition provisions - an economic unit, which may be formed by the parent company and all involved subsidiaries. In accordance with EU law and case-law[182], an undertaking is the economic unit, which engages in commercial/economic activities, regardless of the legal person involved. Therefore, the administrative fines target the whole corporate groups, regardless of the exact entity which infringed the GDPR. Finally, Member State law may impose fines for infringement of other provisions of the GDPR than those mentioned in Article 83, para. 4 - 6[183].

It also should be noted that in case of infringement the DPA may decide not to impose a fine, but one of the measures under Art. 58, for example ban of processing data, suspension of data flows, order for

[180]O'Riordan, John, Bredin, Peter, GDPR: Administrative Sanctions, July 2017, available at: http://www.dilloneustace.com/download/1/Publications/Litigation%20and%20Dispute%20Resolution/GDPR-Administrative%20Sanctions.pdf

[181] Ibid

[182] Case C-41/90 Klaus Höfner and Fritz Elser v Macrotron GmbH

[183] Article 29 data protection working party, Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679, WP 253, p. 7

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

the controller to communicate a personal data breach to the data subject and others. The DPA could also impose both a fine and a measure under Art. 58[184]. After the assessment of the criteria in para. 2, the DPA may decide that in the concrete case breach does not pose a significant risk to the rights of the data subjects concerned and does not affect the essence of the obligation. In such cases, the DPA is allowed, but not obliged, to replace the fine with a reprimand[185].

EU Member States may introduce other penalties, whether criminal or administrative, under their national law, in particular for infringements which are not subject to administrative fines. There is a requirement for these measures to be effective, proportionate and dissuasive.

Key concepts:

Rights of the data subjects: data subjects have the right to lodge a complaint with the DPA, to appeal decisions of the DPA before a court and to complain before a court when the DPA does not comply with its obligations under the GDPR. They can also file a claim and require compensation before a court against a controller or processor where they consider that their rights have been infringed as a result of non-compliance with the GDPR. All these rights could be exercised by a not-for-profit body, organisation or association on behalf of the data subject.

Liability of data controllers and data processors: controllers are liable for all damages caused by processing which infringes the GDPR. Processors bear liability in two cases: when their actions are not compliant with their obligations under the GDPR and when they did not follow lawful instructions of the controller.

Administrative fines: there are two categories of administrative fines depending on the concrete provision that was not complied with. The DPA must determine the size of the fine by taking into account all the factors listed in Art. 83, para. 2, lit. a – k in every separate case.

Most important notions for legal practitioners: legal practitioners must keep up with the national legislation because of the possibility for Member States to impose administrative fines for other

[184] Article 29 data protection working party, Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679, WP 253, p. 7
[185] Ibid

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

infringements than the ones listed in Art. 83. They must also keep in mind the different ways of defending a data subject's rights after an infringement (even if there are no material or non-material damages).

11. Conclusion

This deliverable has shown the variety of applications of the General Data Protection Regulation in the daily practice of the legal practitioners. The report has examined the types of personal data, principles and types of processing, rights of data subjects, legal status of data controller and data processers. All these aspects were analysed in a way to provide a systematic and comprehensive overview of the application of the GDPR, by systemising relevant case law, opinions and guidelines of Article 29 Data Protection Working party, etc.

The broad scope of this Regulation, which brings novelties in both the private and public sector, requires legal practitioners -to be ready to face the challenges that GPDR will introduce. They should keep themselves informed on the developments in relation to the law that shall follow the GDPR and the opinions of both Article 29 Working party, resp. European Data Protection Board and the national guidelines drafted by the respective Data Protection Authority in order to provide adequate legal services to their clients.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

ANNEX

Fundamental principles relating to processing of personal data[186]

In Art. 5 of the GDPR the elementary principles for processing of personal data are determined in an abstract manner for the safeguarding of a high level of protection over the entire Regulation. Such a level of protection requires the application of the European Convention on Human Rights (hereinafter ECHR) requirements in terms of limiting "conditional"[187] fundamental rights, keeping in mind that, where the Charter of Fundamental Rights of the European Union (hereinafter EUCFR) does not offer a stronger protection than the ECHR, the meaning and scope of its provisions are the same of those of the latter[188]. As a result, the GDPR and the Police Directive ensure that each personal data processing act is legally based, pursues a legitimate aim, and is necessary and proportionate to the aim pursued.[189] In this way, the GDPR and the Police Directive standards constitute concretisations of the ECHR (including its Article 8 protecting the right to privacy), of the EUCFR (including its Article 8 protecting the right to personal data protection) and of Art. 16 para. 1 of the Treaty on the Functioning of the European Union (hereinafter TFEU).

In contrast to the former EU Data Protection *Directive*[190] (hereinafter DPD), the general principles of the *Regulation* are now directly applicable pursuant to Art. 288 para. 2 of the TFEU. With this change in the type of legislation comes noticeably an increased relevance of the following principles, since they

[186] This analysis was developed for the INFORM-project by Estelle De Marco (Inthemis, FR) and Matthias Eichfeld (University of Göttingen, DE).

[187] Some of the rights identified in the European Convention on Human rights are called "absolute", such as the right to life or to not be subjected to torture, while others are called "conditional" because they can be subjected to dispensations and/or limitations, as the right to respect for private life and the right to freedom of expression: Frédéric Sudre, 'La dimension internationale et européenne des libertés et droits fondamentaux', *in Libertés et droits fondamentaux*, under the direction of Rémy Cabrillac, Marie-Anne Frison-Roche, Thierry Revet, Dalloz, 11th ed., 2005, pp. 44-45.

[188] EU Charter of Fundamental Rights, article 52, 3.

[189] For further developments regarding the content of the notions of legal basis, legitimate aim, necessity and proportionality, see Estelle De Marco in Estelle de Marco et. al., Deliverable D2.2 – Identification and analysis of the legal and ethical framework, MANDOLA project (Monitoring and Detecting OnLine Hate Speech), GA n° JUST/2014/RRAC/AG/HATE/6652, version 2.2.4 of July 2017, Section 4.1.3, available at http://mandola-project.eu/publications/ (last accessed on 6 December 2017).

[190] Directive 95/46/EC.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

are now **binding in every scenario,** where processing of personal data within the territorial and material scope of the GDPR takes place.[191] In case of their violation claims for damages and sanctions may immediately follow.[192] Even though in numerous articles of the GDPR a certain concretisation of those principles takes place, it is mandatory to consider the fundamental determination in Art. 5 for each act of data processing.

1. Principles of lawfulness, fairness, transparency

Although the three principles standardised in Art. 5 para. 1 lit. a have reciprocal contexts in relation to each other[193], each notion has its own meaning.

1.1. Lawfulness

A personal data processing constitutes a limitation of a fundamental right. As such, such limitation can only be legitimate if it first has a legal basis which must be clear, precise and predictable in its application[194]. This principle is recalled in the GDPR and in the Police Directive, as well as in Directive 95/46/EC. This principle means that the processing must be authorised by law. This law will be in most case the GDPR itself, where processing operations can fully comply with its provisions. But the GDPR provides for cases where an additional legal basis will be required, in order to, *inter alia*, provide for additional safeguards in particular contexts (for example in case of derogations to the provisions of Article 6 and of derogations allowed under Article 23). Where the GDPR constitutes a sufficient legal basis for a given data processing operation, the latter must in addition be based on the consent of the data subject or on any other legitimate basis provided for by law, as foreseen by both Art. 8 para. 2 of the EUCFR. and Article 6 of the GDPR, which provides more specifically for 6 possible legal foundations, including the data subject's consent and the legitimate interests pursued by the controller or by a third party. In order to use the latter legal basis a "test of legitimate interest" must

[191] See *Heberlein*, in: Ehmann/Selmayr, Datenschutz-Grundverordnung, *C.H. Beck*, Munich 2017, Art. 5 para. 1; *Herbst*, in: Kühling/Buchner, Datenschutz-Grundverordnung, *C.H. Beck*, Munich 2017, Art. 5, para. 2; *Frenzel*, in: Paal/Pauly, Datenschutz-Grundverordnung, *C.H. Beck*, Munich 2017, Art. 5 para. 2.
[192] See Art. 82, para. 1 and Art. 83, para. 5 lit. a GDPR.
[193] See Judgement of the CJEU, 1 October 2015, C-201/14 (case "Smaranda Bara"), para. 32 et seq.
[194] See for instance Judgement of the CJEU, 20 May 2003, joined cases C-465/00, C-138/01 and C-139/01 (case "Österreichischer Rundfunk"); Judgement of the ECtHR, 4 December 2008, *Marper*, appl. n° 30562/02 and 30556/04.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

be performed, and in this regards the Article 29 Working Party (becoming the European Data Protection Board in the GDPR)' and GDPR Recital 47 guidelines must be followed.

In addition, specific requirements from the rules governing the lawfulness of the consent[195] and processing of particularly sensitive data must be considered.[196] If there is a transfer of personal data to third countries or international organizations, the specific conditions in Chapter V of the GDPR must be taken into account.[197]

1.2. Fairness

- The principle of fairness has been defined in Directive 95/46/EC as the prohibition of secrecy and the requirement of comprehensive information[198], and the meaning of the principle doesn't seem to have changed. The GDPR adds that, in particular, natural persons should be made aware of the existence of the processing, of the specific purposes for which personal data are processed and of risks, rules, safeguards and rights in relation to the processing of personal data and how to exercise their rights in relation to such processing, as well as of any further information necessary to ensure fairness such as the specific context and circumstances of the processing operations, and the question of whether personal data are mandatory and incurred consequences in case of silence.[199]
- Furthermore, the principle of fairness has been seen by an author as an omnibus clause, which primarily covers situations in which the data subject experiences a disadvantage by processing their personal data, which is not in line with the overall picture of the balance of power between the data subject and the data controller, without necessarily violating a specific legal prohibition.[200] In other words, it enables to ensure transparency as a proportionality safeguard where an imbalance remains between the controller and the data subject, despite the respect

[195] Art. 7 and 8 GDPR.
[196] Art. 9 and 10 GDPR.
[197] Art. 44 to Art. 50 GDPR.
[198] See Recital 38 to Directive 95/46/EC. See also Judgement of the CJEU, 1 October 2015, C-201/14 (case "Smaranda Bara"), para. 34.
[199] See Recital 39 p. 2 et. seq. and Recital 60.
[200] See *Herbst,* in: Kühling/Buchner, op. cit., Art. 5, para. 17; *Frenzel*, in: Paal/Pauly, op. cit., Art. 5 para. 20; *Kramer*, in: Auernhammer, DSGVO – BDSG, *Carl Heymanns Verlag*, Cologne 2017, Art. 5 para. 8-10.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

of the other GDPR requirements.

1.3. Transparency

The principle of transparency adds, to the requirement of fairness or in other words of completeness of the information to be provided, a requirement of clarity of this information (it must be easily accessible, easy to understand, clear and in plain language)[201]. This principle applies to all the information that must be provided in order to ensure a fair and transparent processing.[202] The implementation as a new independent principle (that can be therefore seen as an extension of both the principle of fairness and the obligation of data subject's information) emphasises the importance of transparency as a fundamental proportionality safeguard, and therefore as a fundamental condition for the control over the use of one's own data and thus states a precondition for predictability and thereby effective protection.[203]

As a result, the principles of fairness and transparency concern together both the method and the content of the information.[204]

[201] See Recital 39 to GDPR.
[202] See Recital 58 p. 1 and Recital 39 p. 2. See also Art. 12 para. 1 GDPR.
[203] See Art. 29 Data Protection Working Party, Guidelines on transparency under Regulation 679/2016 (WP 260), p. 5, available at http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083 (last accessed 18 December 2017); see also Commission Staff Working Paper SEC (2012)72 final, Annex 2, Section. 2.4, available at http://ec.europa.eu/justice/data-protection/document/review2012/sec_2012_72_annexes_en.pdf (last accessed on 18 December 2017).
[204] See Art. 12 para. 1; Art. 13 para. 1 and Art. 14 para. 1; see also *Heberlein,* in: Ehmann/Selmayr, op. cit., Art. 5 para. 11.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

2. Principle of purpose limitation[205]

Art. 5 para. 1 lit. b GDPR stipulates that the collection of personal data is only permitted for specific, explicit, legitimate purpose and compatible use.[206]

2.1. Specified purpose

The requirement that the data may only be collected for specified purposes already follows directly from the wording of Article 8 para. 2 EUCFR and from the ECHR principle of necessity (which implies that the rights' limitation - i.e. the processing operations in our context - answers a specific important need -which must be precisely identified and justified-, in addition to be adapted to satisfy this need).

Each purpose must be *"sufficiently defined",* **not later than the time of the data collection**[207], *"to delimit the scope of the processing operation"* and therefore to enable the assessment of the data collection with the law and to enable the *"implementation of any necessary data protection safeguards"*.[208] This specification requires *"an internal assessment"* to identify and detail the kind of processing that *"is and is not included within the specified purpose"*.[209] This means that the controller must not gather data for possible future purposes that are not yet determined at the time of the collection and thus cannot be foreseen by the data subject. Purposes too vague such as *"improving users' experience"* or *"IT-security purposes"* are usually not specific enough.[210] In the same line, an overall purpose to cover a number of separate purposes is not compliant.[211]

---

[205] Some elements of the following discussion are coming from *Estelle de Marco* in: *Estelle de Marco* et. al., Deliverable D2.2 – Identification and analysis of the legal and ethical framework – MANDOLA project (Monitoring and Detecting OnLine Hate Speech), GA n° JUST/2014/RRAC/AG/HATE/6652, version 2.2.4 of July 2017, Section 4.2, p. 68 et seq.: The right to personal data protection, available at http://mandola-project.eu/publications/ (last accessed on 6 December 2017).
[206] Since these notions have already been part of the former DPD, the Article 29 Data Protection Working Party "Opinion 03/2013 on purpose limitation" serves as an adequate reference for further illustration of the principles, as far as no changes are indicated.
[207] See Recital 39 p. 6.
[208] Article 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation (WP 203), 2 April 2013, II.2.1, p. 12 and III.1.1, p. 15 et seq., available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf (last accessed on 6 December 2017).
[209] *Ibid.*, III.1.1, p. 15.
[210] See for more examples *Ibid.*, III.1.1., p. 16.
[211] *Ibid.*, III.1.1, p. 16.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

Only in certain situations, when a detailed description is clearly counter-productive because of its complexity, the specification or the purpose can be reduced to key information.[212] Nevertheless, a detailed description of the processing must be accessible via *"layered notice"* such as a link to a corresponding Internet page.[213]

In addition, since the principle of purpose specification is a practical application of the ECHR principle of necessity (of which weaknesses, in the framework of a complete necessity and proportionality tests, must be balanced by proportionality safeguards), it has to be noted that the performance of a necessity and of a proportionality tests can be used in order to find alternative safeguards that could satisfy data protection authorities and judges, in certain circumstances where the principle of purpose specification cannot be respected as written in the GDPR, such as certain kind of data collection performed in a Big data environment, using specific tools, some of the collected data being used as a second step for specific purposes, where the first motive of the collection can be found legitimate in itself even if too general (such as making profit of a EU based technology aimed at feeding innovative services while avoiding recourses to similar technologies produced in countries where the GDPR does not apply).

2.2. Explicit purpose

The purpose must be *"sufficiently unambiguous and clearly expressed"*[214], *"in such a way to as to be understood in the same way"* by the data controller and its staff including third parties processors, the supervisory authority and the data subjects.[215] This principle enables therefore all the parties *"to have a common understanding of how the data can be used"*, and reduces the risk to process data for a purpose that is not expected by the data subject.[216]In this way it enables data subjects to make informed choices.[217] The important thing is *"the quality and consistency of the information provided"*[218], in addition to its accessibility.

[212] *Ibid.*, III.1.1, p. 16.
[213] Article 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation, op. cit., III.1.1, p. 16.
[214] *Ibid.*, II.2.1, p. 12.
[215] *Ibid.*, III.1.2, p. 17.
[216] *Ibid.*, III.1.2, p. 17.
[217] *Ibid.*, III.1.2, p. 17.
[218] *Ibid.*, III.1.2, p. 18.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

Clearly there is a close relation between the explicit purpose and the principle of transparency and predictability, as these principles all aim to provide the data subject with complete information about the data processing (and at the end to ensure the proportionality of processing operations).[219] Especially for the accountability of the data processor, which Art. 5 para. 2, Art. 24 para. 1 and Art. 30 para. 1 lit. b GDPR require, the determination of an explicit purpose is mandatory.[220]

2.3. Legitimate purpose

As highlighted by the Article 29 Data Protection Working Party, *"the requirement of legitimacy means that* ***the purposes must be in accordance with the law in the broadest sense****. This includes all forms of written and common law, primary and secondary legislation, municipal decrees, judicial precedents, constitutional principles, fundamental rights, other legal principles, as well as jurisprudence, as such 'law' would be interpreted and taken into account by competent courts"*.[221]

2.4. Compatible use

The legal requirement of compatible use responds to the circumstance that it is technically possible to further process data for any purpose, once they have been collected and stored, and thereby interfering repeatedly in the right to protection of personal data. Pursuant to Art. 5 para. 1 lit. b further processing of the collected data is not permitted, if the manner of processing is not compliant with the purpose of the initial collection. It follows from the definition of 'processing' in Article 4 para. 2 GDPR that further processing includes not only the processing of the data for other purposes, but any processing following the collection of the data, which therefore must be compliant with the initial act of collection.[222]

Since the conditions of all principles for the processing of personal data and the requirement of a legal basis for each processing must be fulfilled jointly[223], **two cumulative conditions** must be satisfied:

---

[219] *Ibid*., II.3, p. 13.
[220] See *Heberlein,* in: Ehmann/Selmayr, op. cit., Art. 5 para. 14.
[221] Article 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation, op. cit., III.1.1, p. 20.
[222] This notion of 'further processing' is also established in: Article 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation, op. cit., III.2.1, p. 21: "*any processing following collection, whether for the purposes initially specified or for any additional purposes, must be considered 'further processing' and must thus meet the requirement of compatibility*".
[223] See for the former DPD: Judgement of the CJEU, 1 October 2015, C-201/14 (case "Smaranda Bara"), para. 30 et seq.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

further processing must not be incompatible with the purpose established during the collection of the data and there must be a sufficient legal basis for further processing.[224]

In this context, it is important to note that applying an anonymisation technique constitutes a further processing, which means that such an operation implies on the one hand that the personal data have been first collected in compliance with law, and on the other hand that such an anonymisation needs to be compliant with the fundamental principles (including the need for a legal basis) and the principle of compatible use.[225]

2.4.1 Meaning of recital 50 p. 2 in this context

This interpretation of Art. 5 para. 1 lit. b should also be maintained in the light of Recital 50 p. 2, which, according to its wording, gives the impression that there is no requirement for a separate legal basis in case of a compatible change of purpose. If that were the case, Article 5 para. 1 lit. b in combination with the wide criteria of Art. 6 para. 4 would have the character of a general clause-like extension of all legal bases of Article 6 para. 1.

Against such an understanding of the recital argues that the assessment of the purpose compatibility represents an additional **limiting criterion**, which was already established in similar terms in the former DPD.[226] Since there is no indication in the GDPR except for the wording in recital 50 p. 2 for such a new understanding of the principle of compatible use, the wording can only be understood as meaning that no new legal basis is required if the subsequent processing involves the execution of the

---

[224] Article 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation, op. cit., III.2.1, p. 21; III.2.3., p. 33; See furthermore Article 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation, op. cit., II.2.1, p. 12, fn. 28: "*Article 8 (2) of the Charter also makes it clear that the requirement of purpose specification is a separate, cumulative requirement that applies in addition to the requirement of an appropriate legal ground.*"; See also *Heberlein,* in: Ehmann/Selmayr, op. cit., Art. 5 para. 19; *Herbst,* in: Kühling/Buchner, op. cit., Art. 5, para. 42.

[225] Art. 29 Data Protection Working Party, Opinion 05/2014 on Anonymization Techniques (WP 216), 10 April 2014, 2.2.1, p. 7, available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf (last accessed on 6 December 2017).

[226] Following the rapporteur of the EU-Parliament involved in the trilogue negotiations *Jan Philipp Albrecht*: *Albrecht*, Das neue EU-Datenschutzrecht – von der Richtlinie zu Verordnung, Überblick und Hintergründe zum finalen Text für die Datenschutz-Grundverordnung der EU nach der Einigung im Trilog, in: Computer und Recht 2016, 88 (92); See furthermore the assessment of state council and desk officer of the German Ministry of Justice and Consumer Protection *Peter Schantz*: *Schantz*, Die neue Datenschutz-Grundverordnung – Beginn einer neuen Zeitrechnung im Datenschutzrecht, in: Neue Juristische Wochenschrift 2016, 1841 (1844); See also *Herbst,* in: Kühling/Buchner, op. cit., Art. 5, para. 49; *Buchner/Petri* in: Kühling/Buchner, op. cit., Art. 6, para. 182 et seq.; *Heberlein,* in: Ehmann/Selmayr, op. cit., Art. 5 para. 20.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

initial processing and meets the conditions of the legal basis for the initial processing. A different interpretation of recital 50 p. 2 would be incompatible with the principle of lawfulness of Art. 5 para. 1 lit. a and the overall protective purpose of the GDPR, which is stated in Art. 1 para. 2.[227]

2.4.2 Key factors for purpose compatibility assessment

For further processing, in addition to the existence of a new corresponding legal basis, a detailed examination of the compatibility of the purposes has to be carried out. According to Art. 6 para. 4, the test is mandatory where "the processing for a purpose other than that for which the personal data have been collected is not based on the data subjects consent or on a Union or Member State law[228]".

This determination is followed by a non-exhaustive list of criteria for such a process, which is essentially based on the factors developed by the Art. 29 Data Protection Working Party.[229]

- *Any link between the purposes for which the data have been collected and the purposes of further processing, Art. 6 para. 4 lit. a:*

  The issue is to analyse the 'substance' of this relationship, to notably determine if the further processing was "*already more or less implied in the initial purposes, or assumed as a logical next step in the processing according to those purposes*", or if there is only a "*partial or even non-existent link with the original purposes*".[230]

  Although the compatibility requirement is usually missing between the processing for a purpose of a contract and the notice of potential criminal offenses or any potential public security threat given by the data controller to the competent authorities, in such a case there is a legitimate interest of the data controller (Art. 6 para. 1 lit. f) for the display and transmission

[227] See *Heberlein,* in: Ehmann/Selmayr, op. cit., Art. 5 para. 20; *Herbst,* in: Kühling/Buchner, op. cit., Art. 5, para. 49.
[228] Such a law must protect the important public interests referred to in Article 23 para. 1 of the GDPR, the data subject or the rights and freedoms of other persons and must comply with the proportionality test required by Article 52 para. 1 of the EUCFR and Article 8 of the ECHR. See Judgement of the CJEU, 6 October 2015, C-362/14 (case "Schrems"); Judgement of the CJEU, 8 August 2014, C-293/12 (case "Digital Rights Ireland").
[229] Article 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation, op. cit., III.2.1, p. 21; III.2.2, p. 23 et seq.; The GDPR lists five principles but two of them are handled under the same one by the Article 29 Data Protection Working Party.
[230] Article 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation, op. cit., III.2.2, p. 23 et seq.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

of personal data.[231] Of course, this does not apply if the data controller is subject to a confidentiality obligation.[232]

- *The context in which the data have been collected, Art. 6 para. 4 lit. b:*

  This assessment should be based, above all, on the 'reasonable expectations' of the data subject resulting from the relationship with the data controller.[233] The more surprising and unpredictable further processing is for the data subject, the more indicates to an incompatibility with the original purpose.[234] For instance, it is incompatible to use security monitoring to control workers, a breathalyser to check working hours or to collect fingerprints of asylum seekers for the initial purpose of prevention from filling multiple asylum applications in different member states simultaneously but using them for law enforcement purposes later on.[235]

- *The nature of the personal data, Art. 6 para. 4:*

  This criterion refers especially to the further processing of special categories of personal data (Art. 9) or personal data related to criminal convictions and offences (Art. 10), but also communication data, location data or whether the data subject is a child or belongs to a more vulnerable segment of the population requiring special protection.[236] As a result, a particularly careful examination is necessary.[237] As well, the general principles and the special requirements for the protection of sensitive data must be considered in such a further processing.[238]

- *The possible consequences of the intended further processing for the data subject, Art. 6 para. 1 lit. d:*

[231] Recital 50 p. 9.
[232] Recital 50 p. 10.
[233] Recital 50 p. 6.
[234] Article 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation, op. cit., III.2.2, p. 24.
[235] Article 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation, op. cit., Annex 4, p. 56 et seq., 68.
[236] Article 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation, op. cit., III.2.2, p. 25, fn. 68.
[237] *Ibid.*
[238] Recital 50 p. 8.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

Both positive and negative consequences must be taken into account for the assessment.[239] According to the risk-based approach of the GDPR (Art. 24 para. 1), potential risks must be included such as the publication of the data or other making accessible to a larger group of people, the processing by third parties or whether a combination with other data takes place.[240] This applies especially if there is a risk of discrimination or damage to the reputation of the data subject.[241]

- *The existence of appropriate safeguards, Art. 6 para. 4 lit. e:*

  Such as in a proportionality test, appropriate safeguards need to be implemented in order to ensure both (1) that the freedoms' limitation will not be higher than the one that has been assessed (through ensuring that the context, conditions and content of the intended processing will not be modified - including protection mechanisms already implemented), and (2) that weaknesses identified during first steps of the compatibility test and compensated. These safeguards may consist in the first place in technical and/or organisational safeguards ensuring *inter alia* anonymisation each time this is possible[242] or "functional separation", which includes the consideration of, encryption and pseudonymisation[243] techniques and of aggregation techniques[244], in other words the consideration of measures ensuring that the "*data cannot be used to take decisions or other actions with respect to individuals*"[245]). These safeguards may also consist in ensuring transparency (including purpose re-specification) and data subjects' control (collection of users' new consent, opt-out possibilities, data subjects' rights…)[246].

[239] Article 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation, op. cit., III.2.2, p. 25.
[240] *Ibid.*,
[241] Recital 75.
[242] See for example Recital 39 of the GDPR; Article 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation, op. cit., III.2.2, p. 27
[243] See the Definition in Art. 4 No. 5.
[244] Article 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation, op. cit., III.2.2, p. 27.
[245] *Ibid.*
[246] *Ibid.*

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

2.4.3 Compatible use in case of privileged purposes

According to Art. 5 para. 1 lit. b archiving purposes, scientific or historical research purposes or statistical purposes are considered as privileged purposes, which means that there is a presumption of conformity for such a purpose. However, the lawfulness of the further processing for these purposes presupposes that it complies with the conditions laid down in Article 89 para. 1. The latter provides for appropriate guarantees for this process which may be supplemented and specified in the form of member state legislation.[247] Amongst those guarantees, lies the requirement to perform a compatibility test in order to identify all safeguards that are appropriate to the specific context[248]. Besides, any such processing must of course also comply with all the fundamental principles of Art. 5[249] and more generally with all the other requirements of the GDPR, including the requirement to be based on one of the grounds listed in Article 6 para 1 of the GDPR[250] and the requirement to inform the data subject of the processing' purposes and of his or her rights.[251]

3. Principle of data minimisation

Art. 5 para. 1 lit. c states that the processed data must be "*adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed*". According to this principle, personal data may only be processed if the purpose of the processing cannot be reasonably achieved by other means.[252] This includes the implementation of anonymisation techniques if possible, which would cease the personal

[247] Art. 89 para. 2 and 3.
[248] This requirement has been highlighted by the Article 29 Data Protection Working Party (Opinion 03/2013 on purpose limitation, *op. cit.* III.2.3, p.28) in relation to Article 5 of Directive 95/46/EC. However, it is also applicable in the context of the GDPR since its Article 5 refers to Article 89, which requires the implementation of "safeguards (that must be) "*appropriate (...), in accordance with this Regulation*" (while the Directive required the provision of appropriate safeguards). Safeguards proposed in Article 89 of the GDPR are only elements of a proposed list that must be complemented by all the safeguards that are appropriate in the specific context.
[249] Recital 50 p. 8.
[250] Article 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation, *op. cit.*, III.2.3, p.28. This opinion has been delivered in relation to Article 6b of Directive 95/46/EC. However, the formulation of Article 5 of the GDPR being almost the same, this decision appears to be applicable in this context too.
[251] Recital 50 p. 8.
[252] Recital 39 p. 9.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

reference and thus the data would be no longer subject to data protection law.[253] Obviously, there is a close relation to the principle of time limitation for data storage. A specification of this principle takes place, inter alia, in the concepts of privacy by design and by default in Art. 25.

4. Principle of accuracy

According to Art. 5 para. 1 lit. d personal data must be "*accurate and, where necessary, kept up to date*". To ensure the data quality, the data controller must actively take every "*reasonable step*" to rectify or delete inaccurate data without delay.[254] Since the usage of personal data might produce legal consequences for the data subject, the data shall reflect reality at any given time.[255] To enforce this principle, the data subject has the right to rectification (Art. 16) and the right to erasure (Art. 17).

It is important to notice that this obligation must be complied especially with respect to the purposes and the specific circumstances of processing.[256] For instance, if the processing purpose is preservation of evidence it can be necessary to process outdated data.[257]

5. Principle of storage time limitation

Art. 5 para. 1 lit. e determines that the storage period of personal data should be kept to a 'strict minimum'.[258] Decisive for the permissible duration of storage is the purpose of the processing. Thus, the principle of storage time limitation is an application of the principle of proportionality defined in terms of time. In order to preserve this principle, it is sufficient to remove the personal reference of the data (identifiability) according to the wording in Art. 5 para. 1 lit. e.[259]

To ensure the concept of limitation the data controller should establish time limits for erasure and for a periodic review.[260] Pursuant to Art. 13 para. 2 lit. a, Art. 14 para. 2 lit. a and Art. 15 para. 1 lit. d the

[253] See *Herbst,* in: Kühling/Buchner, op. cit., Art. 5, para. 58; See for the procedure of anonymization: Art. 29 Data Protection Working Party, Opinion 05/2014 on Anonymization Techniques, op. cit., 2.2.1, p. 7 et seq.
[254] Art. 5 para. 1 lit. d; Recital 39 p. 11.
[255] See *Voigt/von dem Bussche*, in: Voigt/von dem Bussche, The EU General Data Protection Regulation (GDPR) – A Practical Guide, *Springer*, Cham (Switzerland) 2017, 4.1.4, p. 91; *Frenzel*, in: Paal/Pauly, op. cit., Art. 5 para. 39.
[256] Art. 5 para. 1 lit. d.
[257] See *Heberlein,* in: Ehmann/Selmayr, op. cit., Art. 5 para. 24; *Frenzel*, in: Paal/Pauly, op. cit. Art. 5 para. 40 et seq.
[258] Recital 39 p. 8.
[259] See Recital 26 p. 3 and 4 for further explanations on the criterion of identifiability.
[260] Recital 39 p. 10.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

data controller must inform the data subject of the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period. To enforce this principle, the data controller is obliged to erase personal data under the provision of Art. 17.

Similar to the constitution of privileged purposes in Art. 5 para. 1 lit. b, there are exceptions to the principle of storage time limitation as well. If the personal data is processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, the storage for a longer period is explicitly allowed.[261] In such a case, appropriate guarantees in accordance with Art. 89 para. 1 are required.

6. Principle of integrity and confidentiality

According to Art. 5 para. 1 lit. f processing must be carried out "in a manner that ensures adequate security of personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures".[262]

In this way, the principle addresses the need for organisational safeguards for the processing operation. Specifications of the protective measures especially take place in Art. 32, Art. 28 para. 2 p. 2 lit. b and Art. 29.[263] Moreover, personal data breaches must be reported to the supervisory authority (Art. 33) and, in certain situations, to the data subject (Art. 34).

7. Accountability

The data controller is responsible for and must be able to **demonstrate compliance with the fundamental principles** relating to processing of personal data, Art. 5 para. 2.[264] The extended obligation of accountability is an expression of the enhanced self-responsibility of the data controller under the GDPR.

[261] Art. 5 para. 1 lit. e.
[262] See also recital 39 p. 12.
[263] For further explanations to the concrete nature and extent of adequate protective measures see the sections of the specific obligations of data controller and data processor.
[264] See for the notion also Article 29 Data Protection Working Party, Opinion 03/2010 on the principle of accountability (WP 173), 13 July 2010, III.2, p. 9 et. seq., available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2010/wp173_en.pdf (last accessed on 15 December 2017).

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

7.1 Liability of the data controller or data processor

Irrespective of the possibilities of the data subject for remedy against the processing activity of the data controller (Art. 77-79), any infringement of the regulation may lead to a claim for compensation of damage caused by processing, unless the controller or the processor has complied with the obligations of the regulation, Art. 82.

7.2 Accountability and data protection by design and by default[265]

A specification of the notion of self-responsibility takes place in Art. 24 which requires of the data controller to "implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with" the regulation, "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". As recital 75 phrase 2 points out, this can be done by having the data controller adopt internal strategies and take measures that comply with the principles of data protection by design and by default (Art. 25 para. 1 and 2).

In any case the data controller must ensure accountability by keeping a record of processing activities (Art. 30), cooperating with supervisory authorities (Art. 31), reporting and notification of data breaches (Art. 33, 34), carrying out a data protection impact assessment in certain situations (Art. 35) and the corresponding prior consultation of the supervisory authority (Art. 36).

The overall responsibility and accountability of the data controller include the responsibility for the processing of the data processor (who is acting on behalf of the data controller).[266] Nevertheless, the processor is also demanded to take appropriate technical and organisational measures to take care of the risk associated with data processing.[267]

[265] For further explanations on the concept of accountability see the sections of the specific obligations of data controller and data processor.
[266] Art. 28 para. 1.
[267] Art. 32 para. 1.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

8. Prohibition of automated decision-making

Not in Art. 5 but in Art. 22 of the GDPR the right of the data subject is stated, "*not to be subject to a decision solely based on automated processing, including profiling, which produces legal affects concerning him or her or similarly significantly affects him or her*". From the perspective of the data controller, this determination leads in turn to the fact that there is a prohibition on fully automated decision-making that has a legal or similarly significant effect concerning the data subject.[268] A decision is based solely on automated processing if there is no human involvement and the outcome of the processing is not reviewed by a competent and authorised person.[269] The intention is that the data subject shall have the right to a final decision by a human being if the decision implies an increased risk for his or her situation.[270]
The wording of Art. 22 para. 1 and the complementary recital 71 indicate a narrow interpretation of 'similarly significant effects', since it is in a close context to 'legal affects'. According to the Art. 29 Data Protection Working Party it depends upon the characteristics of each case, including:

- the intrusiveness of the profiling process;
- the expectations and wishes of the individuals concerned;
- the way the advert is delivered; or
- the particular vulnerabilities of the data subject targeted.[271]

As a result, certain practices of targeted online advertising may have such an effect, especially when it comes to differential pricing strategies.[272]

There are three exceptions to the prohibition listed in para. 2 of Art. 22: If the automated-decision making is necessary for the performance of a contract between data controller and data subject, if there

[268] See Art. 29 Data Protection Working Party, Guidelines on automated individual decision-making and Profiling for the purposes of Regulation 679/2016 (WP 251), 3 October 2017, II., p. 9, available at http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083 (last accessed 18 December 2017).
[269] *Ibid.*, II.A., p. 9 et seq.; See also *Schrey*, in: Rücker/Kugler, New European General Data Protection Regulation – A Practitioner's Guide, *Nomos, C.H. Beck, Hart*, Baden-Baden, Munich and Oxford 2017, p. 149, para. 692.
[270] See Art. 29 Data Protection Working Party, Guidelines on automated individual decision-making and Profiling for the purposes of Regulation 679/2016., op.cit., II.B., p. 10 et seq.
[271] *Ibid.*, II.B., p. 11.
[272] *Ibid.*

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

is an authorisation provided by Union or Member State law or if the data subject has given his or her explicit consent. Regarding special categories of data (Art. 9 para. 1) the exceptions for automated decision-making are not applicable, unless the conditions of Art. 9 para. 2 lit. a or g are met. In all cases, it is necessary to "*implement suitable measures to safeguard data subject's rights and freedoms and legitimate interests*"[273].

[273] Art. 22 para. 2 lit. b, para. 3, para. 4.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

Bibliography

Charter of Fundamental Rights of The European Union 2012/C 326/02

European Convention on Human Rights

Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

Treaty on the Functioning of the European Union

Case C-550/07 P Akzo Nobel Chemicals Ltd and Akcros Chemicals Ltd v European Commission

Case Case C-41/90 Klaus Höfner and Fritz Elser v Macrotron GmbH

ECJ, Judgement on Case C-28/08 P, *European Commission v the Bavarian Lager Co. Ltd*, of 29 June 2010,

Judgement of Case C-73/07, *Tietosuojavaltuutettu v Satakunnan Markkinapörssi Oy, Satamedia Oy*, 16 December 2008

Judgement of the CJEU, 1 October 2015, C-201/14 (case "Smaranda Bara").

Judgement of the CJEU, 20 May 2003, joined cases C-465/00, C-138/01 and C-139/01 (case "Österreichischer Rundfunk")

Judgement of the ECtHR, 4 December 2008, *Marper*, appl. n° 30562/02 and 30556/04.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

Art. 29 Data Protection Working Party, Guidelines on automated individual decision-making and Profiling for the purposes of Regulation 679/2016 (WP 251), 3 October 2017, available at http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083

Article 29 Data Protection Working Party, Opinion 05/2014 on Anonymization Techniques (WP 216), 10 April 2014, available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf (last accessed on 6 December 2017).

Article 29 data protection working party, Guidelines on the application and setting of administrative fines for the purposes of the Regulation 2016/679, WP 253, adopted on 3 October 2017

Article 29 Data Protection Working Party, Guidelines on Transparency

Article 29 Data Protection Working Party, Opinion 03/2010 on the principle of accountability (WP 173), 13 July 2010, available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2010/wp173_en.pdf

Article 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation 2 April 2013, available at http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf

Article 29 Data Protection Working Party, Opinion 1/2010 on the concepts of "controller" and "processor", adopted on 16 February 2010, WP169

Article 29 Working Party, Opinion 4/2007 on the concept of personal data of, adopted on 20 June 2007, available at: https://www.clinicalstudydatarequest.com/Documents/Privacy-European-guidance.pdf

Article 29 Working Party, Guidelines on Article 49 of Regulation 2016/679, WP262

Article 29 Working party, Guidelines on Consent under Regulation 2016/679, adopted on 28.11.2017, WP259

Article 29 Working Party, *Guidelines on Data Protection Officers ('DPOs')*, adopted on 13 December 2016

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

Article 29 Working Party, Working Document on the processing of personal data relating to health in electronic health records (EHR), WP131

Ausloos, Jef, *Balancing in the GDPR: legitimate interests v. right to object*, 28 February 2017, available at: https://www.law.kuleuven.be/citip/blog/balancing-in-the-gdpr-legitimate-interests-v-right-to-object/

Ausloos, Jef, *The Interaction between the Rights to Object and to Erasure in the GDPR*, 25 August 2016, https://www.law.kuleuven.be/citip/blog/gdpr-update-the-interaction-between-the-right-to-object-and-the-right-to-erasure/

Baker & McKenzie LLP, *Accountability Obligations under the GDPR*, available at http://globalitc.bakermckenzie.com/files/Uploads/Documents/Global%20ITC/13%20Game%20Changers/BM-Accountability%20Obligations%20under%20the%20GDPR.pdf

Bergt M, *Die Bestimmbarkeit als Grundproblem des Datenschutzrechts – Uberblick über, den Theorienstreit und Losungsvorschlag*, 2015

Bolgar, Peter, Kelly, Jeanne, Enforcement and Remedies under the GDPR, 18 September 2017, available at: https://www.lexology.com/library/detail.aspx?g=35f640a4-0a8a-4a81-becb-392fcb201042

Carl Heymanns Verlag, Cologne 2017

Commission Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data, COM (2012) 11 final; 2012/0011 (COD)

Commission Staff Working Paper SEC (2012)72 final, available at http://ec.europa.eu/justice/data-protection/document/review2012/sec_2012_72_annexes_en.pdf (last accessed on 18 December 2017

Estelle De Marco in Estelle de Marco et. al., Deliverable D2.2 – Identification and analysis of the legal and ethical framework, MANDOLA project (Monitoring and Detecting OnLine Hate Speech), GA n°

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

JUST/2014/RRAC/AG/HATE/6652, version 2.2.4 of July 2017, available at http://mandola-project.eu/publications/ (last accessed on 6 December 2017)

EU Agency for Network and Information Security, *Privacy and Data Protection by Design*, December 2014

Foitzik, Piotr, How to comply with provisions on joint controllers under the GDPR, 26 September 2017, available at: https://iapp.org/news/a/how-to-comply-with-provisions-on-joint-controllers-under-the-gdpr/

Frenzel, in: Paal/Pauly;

Gabel, Detlev, Dr., Hickman, Tim, Remedies and sanctions – Unlocking the EU General Data Protection Regulation, 22 July 2016, available at: https://www.whitecase.com/publications/article/chapter-16-remedies-and-sanctions-unlocking-eu-general-data-protection

Hansen M, *Data Protection by Default – Requirements, Solutions, Questions*, IPEN Workshop, Vienna, 9 June 2017, p. 4, available at: https://edps.europa.eu/sites/edp/files/publication/17-06-09_marit_hansen-dataprotectionbydefault_ipen-workshop_vienna_hansen_en.pdf

Heberlein, Ehmann/Selmayr,

Heberlein, Ehmann/Selmayr, Datenschutz-Grundverordnung, *C.H. Beck*, Munich 2017

Heimes, Rita, Top 10 operational impacts of the GDPR: Part 1 – data security and breach notification, 06 January 2016, available at: https://iapp.org/news/a/top-10-operational-impacts-of-the-gdpr-part-1-data-security-and-breach-notification

Herbst, Kühling/Buchner,

Herbst, Kühling/Buchner, Datenschutz-Grundverordnung, *C.H. Beck*, Munich 2017

Hon, W Kuan, Dr., Data Protection: Controllers, Processors, Contracts, Liability – the ICO Draft Guidance, 06 October 2017, available at: https://www.scl.org/articles/10017-data-protection-controllers-processors-contracts-liability-the-ico-draft-guidance

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

ICO Guide, *"Determining what information is 'data' for the purposes of the DPA"*, available on https://ico.org.uk/media/for-organisations/documents/1609/what_is_data_for_the_purposes_of_the_dpa.pdf

ICO Guide, Data controllers and data processors: what the difference is and what the governance implications are, available at: https://ico.org.uk/media/for-organisations/documents/1546/data-controllers-and-data-processors-dp-guidance.pdf

ICO Guide, Do all organisations need to document their processing activities?, available at: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/documentation/who-needs-to-document-their-processing-activities/

ICO guide, Lawful basis for processing, available at: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/contract/

ICO Guide, Right of access, available at: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-of-access/

ICO Guide, Right of restriction, https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-restrict-processing/

ICO, *The Guide to Data Protection*, available at https://ico.org.uk/media/for-organisations/guide-to-data-protection-2-9.pdf

Kenny S, *An Introduction to Privacy Enhancing Technologies*, IAPP, The privacy advisor, available at https://iapp.org/news/a/2008-05-introduction-to-privacy-enhancing-technologies/

Kramer, Auernhammer, DSGVO – BDSG,

O'Riordan, John, Bredin, Peter, GDPR: Administrative Sanctions, July 2017, available at: http://www.dilloneustace.com/download/1/Publications/Litigation%20and%20Dispute%20Resolution/GDPR-Administrative%20Sanctions.pdf

O'Rorke, Owen, Under control?, 4 July 2017, available at: http://communities.lawsociety.org.uk/law-management/magazine/july-2017/under-control/5062090.fullarticle

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

Opinion of Advocate General Campos Sanchez-Bordona, delivered on 12 May 2016 in Case C-582/14, *Patrick Breyer v Bundesrepublik Deutschland*

Opinion of Advocate General Kokott, delivered on 20 July 2017 in Case C-434/16, *Peter Nowak v Data Protection Commissioner*,

Reed C., *"Taking Sides on Technology Neutrality"*, 2007, 4(3) SCRIPT-ed

Room S., *Security of Personal Data* in *European Data Protection Law and Practice*, IAPP publication, 2018

Springer, Cham (Switzerland) 2017

The Law Society, Appointment of data protection officers by law firms. General Data Protection Regulation guidance, 2018

Van Canneyt, Tim, Provoost, Soo Mee, Belgian DPA publishes recommendation on GDPR record keeping obligation, 4 July, 2017

Voigt P., *Datenschutz bei Google*, MMR, 2009

Von dem Bussche A., Voigt P., *The EU general data protection regulation (GDPR). A practical guide*, Springer International Publishing, 2017

Zomorodi M, Poyant J, Aaron K, *Privacy Paradox: What You Can Do About Your Data Right Now*, available at: https://www.npr.org/sections/alltechconsidered/2017/01/30/512434746/privacy-paradox-what-you-can-do-about-your-data-right-now

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.