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

D2.1 Review report of GDPR with respect to judiciary

Lead partner: ITTIG-CNR

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: Ginevra Peruginelli, Sara Conti and Sebastiano Faro, ITTIG-CNR Matthias Eichfeld, University of Göttingen	16/01/2018
Version 1	Reviewed by: Matthias Eichfeld, University of Göttingen	27/02/2018
Version 1	Reviewed by: George Dimitrov, Law and Internet Foundation	01/03/2018
Version 1	Reviewed by: Matthias Eichfeld, University of Göttingen	01/03/2018
Version 2	Updated by: Ginevra Peruginelli, Sara Conti and Sebastiano Faro, ITTIG-CNR	09/03/2018
Version 2	Reviewed by: George Dimitrov, Law and Internet Foundation	12/03/2018

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

The subject of this study are the requirements that will be put forward by the implementation of the GDPR to the data processing in the judiciary. First of all, a definition of the term *judiciary* is taken in order to be able to respond as specifically as possible to the respective data processing activities and also to make a meaningful distinction with regard to the other target groups of the INFORM project (legal practitioners, court staff). In the next step, the scope of application of the GDPR is scrutinized, especially taking in account recital 20, which is of particular relevance to the judiciary. In the following, the data processing activities of the judiciary are analysed in the light of the GDPR and a classification of the activities is made under the position of the data controller and data processor. Above all, the perspective of the data controller proves to be crucial for the judiciary. After presenting the basic principles of data processing for the framework of the INFORM project, the central legal bases for the judiciary are discussed. Afterwards, the extensive duties of the data controller are described, which must be considered in every data processing. The starting point is the characterisation of the risk-based approach, which is an essential aspect of the GDPR and gets reflected for instance in the determination of sufficient data security. The extent to which the data processor also needs to fulfil the corresponding obligations is explained afterwards. Finally, an overview of the much-extended fines standard of the GDPR in comparison to the former Data Protection Directive is provided, which, however, will probably not directly affect the judiciary as a public body.

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

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.

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.

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.

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: Scope and definition of the judiciary

For the purpose of the present review report on GDPR aimed at the judiciary it is necessary to define the scope and give a specific notion of this target group tailored to the INFORM project.

Legal and judicial cultures across Europe are diverse. In particular, the concept of judiciary does not refer to a clearly defined or widely accepted concept. Also known as "judicial system" or "court system" the specific meaning of judiciary depends on the context in which it occurs.

There are many definitions of judiciary, all strictly related to the concept of justice and to its dictates in various fields of life as well as to the implications of injustice.

The judiciary is the body trusted to maintain public order; it ensures conformity of the law to the principles of the basic law and it administers the law within this framework[1]. The judiciary can also be defined as the section of government that is responsible for the settlement of law. The concept is strictly related to the following terms:

- Court as the system of courts that interprets and applies the law.
- Jurisdiction as the official authority making legal decisions and judgements over an individual or materialistic item within a territory. The term "jurisdiction" comes from *juris* and *diction.*

From the operative point of view the concept also refers collectively to the personnel, such as judges, magistrates and other adjudicators, who form the core of a judiciary, as well as the staff who keeps the system running. Within this approach, it is useful to distinguish different concepts[2]:

1. A Court is defined as a "body established by law and appointed to adjudicate on specific type(s) of judicial disputes within a specified administrative structure where one or several judge(s)

[1] Pikēs, Geōrgios, *Justice and the judiciary*. Leiden; Boston: Martinus Nijhoff Publishers, 2012.
[2] European Commission for the *Efficiency* of *Justice (*CEPEJ), *Report on "European judicial systems –Edition 2014 (2012 data): efficiency and quality of justice*", Council of Europe, 2012

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/are sitting on a temporary or permanent basis"[3].

A distinction is made between:

- first instance courts of general jurisdiction (legal entities): these courts deal with those issues which are not attributed to specialised courts according to the nature of the case,
- first instance specialised courts (legal entities),
- all courts considered as geographical locations: these are premises or court buildings where judicial hearings take place.

Courts perform different tasks according to the competences assigned by law. In the majority of cases, courts are responsible for dealing with civil and criminal law cases, and possibly administrative matters. Furthermore, courts may have a responsibility for the maintenance of registers and have special departments for enforcement cases.

Judiciary branches can host public legal professionals and institutions: this happens in most EU countries where prosecutors, state lawyers, ombudsmen, public notaries, judicial police service and legal aid officers give their contribution. The judicial administration governing courts sometimes also governs these institutions, and, in some cases, the administration of the judicial branch is also the administering authority for private legal professions such as lawyers and private notary offices.

2. A judge is a person entrusted with giving, or taking part in, a judicial decision opposing parties who can be either legal or natural persons, during a trial. In particular, "the judge decides, according to the law and following an organised proceeding, on any issue within his/her jurisdiction"[4].

Three types of judges can be envisaged:

- professional judges who have been trained and work as a judge and not as a prosecutor;

[3] European Commission for the *Efficiency of Justice, cit.*, p. 112
[4] European Commission for the *Efficiency* of *Justice, cit.*, 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.

- professional judges who practice on an occasional basis and are paid as such;
- non-professional judges who are volunteers: they are compensated for their expenses and give binding decisions in courts.

3. The prosecutors. In Recommendation Rec(2000)19 on the Role of Public Prosecution in the Criminal Justice System, adopted by the Committee of Ministers of the Council of Europe on 6 October 2000, prosecutors are defined as: "public authorities who, on behalf of society and in the public interest, ensure the application of the law where the breach of the law carries a criminal sanction, taking into account both the rights of the individual and the necessary effectiveness of the criminal justice system"[5]. The prosecution function is organised differently by States where a public authority is charged to carry out prosecutions. It can be noted that, while the role of the judge seems to be relatively homogeneous in the States or entities, that of the prosecutor is much less so. In all European States or entities, prosecutors play an important role in the prosecution of criminal cases. In most of the States or entities, they also have a responsibility in the civil and even administrative law area. Another important aspect to be taken into account relates to the different levels of autonomy of public prosecutors. In some States or entities, they benefit from protection of their independence on an equal level with judges, while in other States or entities, the criminal policies are directed from the Ministry of Justice and the level of independence is limited. In some States or entities (for example, Denmark, Greece, Malta, Poland, UK England and Wales, Israel), specially authorized police officers have prerogatives during the preparatory phase before trial, or even in conducting the prosecution, held exclusively by public prosecutors in other states. Another important difference concerns prosecutors' membership of the judiciary: in countries where the justice system is based on or influenced by common law, prosecutors are not considered to be part of the judiciary, whereas in Nordic countries they are effectively part of the judiciary.

[5] Council of Europe: Committee of Ministers, *Recommendation Rec(2000)19 of the Committee of Ministers to Member States on the Role of Public Prosecution in the Criminal Justice System,* 6 October 2000, Rec(2000)19, available at: http://www.refworld.org/docid/43f5c8694.htm

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. Staff in courts. Five types of non-judicial staff can be identified:

- the "Rechtspfleger" are high-ranking judicial officials to whom judicial tasks have been transferred in order to perform these tasks independently and to decide objective independent. They belong to the higher service in court. The court officials, who are similar to the Rechtspfleger, can be charged of judicial tasks so that they act independently and can also give their contribution in judicial proceedings alongside the judge, without assisting him. The "Rechtspfleger falls between judges and non-judge staff, like registrars. He/she may carry out various legal tasks, for example in the areas of family or succession law and has competence to make judicial decisions independently on various matters such as the granting of nationality, payment orders, execution of court decisions, auctions of immovable goods, criminal cases, enforcement of judgements in criminal matters; and can undertake administrative judicial tasks. Therefore, when they are acting in their judicial capacity, they should be considered as part of the judiciary. When they are acting in their administrative capacity, they should be considered as part of the court staff[6]. The European Union of Rechtspfleger (E.U.R.) represents the profession of Rechtspfleger and comparable higher officials in Europe;

- non-judicial staff whose task is to assist judges directly (case file preparation, assistance during the hearing, court recording, helping to draft the decisions) such as registrars. Both judicial advisors and registrars assist;

- staff responsible for various administrative matters and for court management; human resources management, material and equipment management, including computer systems, financial and budgetary management, training management;

- technical staff responsible for IT equipment, security…;

[6] More information on Rechtspfleger's responsibilities in relation to data processing acting in administrative capacity could be found in D2.7 Review report on GDPR aimed at court staff 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.

- other non-judicial staff.

5. Staff attached to the public prosecution services

As in the case of judges, public prosecutors are assisted by staff performing widely varying tasks such as secretariat, research, case preparation, or assistance in the proceedings. The law may also entrust to non-prosecutor staff (Rechtspfleger or its equivalent) some functions of the prosecution.

1.1. The linguistic analysis

The term judiciary is not always clear and unequivocal. The etymology of the term judiciary is the following: "relating to courts," early 15c., from Latin *iudiciarius* or belonging to a court of justice, from *iudicium* "judgment, court of justice," from *iudicem* "a judge". The noun meaning referring to "a body of judges, judges collectively" is from 1788 (judicature was used in this sense from 1590s).

On the basis of a brief analysis conducted through the European Union's terminology *database IATE (*"Inter-Active Terminology for Europe) the following table of the translation of the term judiciary in different EU languages is shown.

POLITICS, LAW

EN	**judiciary**
	courts
	judicial system
	judicature
BG	съдебна власт
CS	soudnictví
	soudní moc

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.

DA	dømmende magt
	dommerstand
	dommere og anklagere
DE	Justiz
	Gerichtsbarkeit
	Richter und Staatsanwälte
EL	δικαστικό σώμα
ES	carrera judicial
	poder judicial
	judicatura
FI	lainkäyttö
	tuomioistuimet
	lainkäyttöjärjestelmä
	oikeuslaitos
FR	pouvoir judiciaire
	corps judiciaire
	magistrature
GA	na breithiúna

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.

HU	igazságszolgáltatás
IT	potere giudiziario
	corpo giudiziario
	magistratura
LT	teisminės institucijos
LV	tiesu vara
	tiesneši
	tiesu iestādes
MT	ġudikatura
NL	rechterlijke macht
	gerechtelijk apparaat
	rechterlijk college
PL	sądownictwo
PT	poder judicial
	corpo judicial
	sistema judiciário
SK	justícia
	súdnictvo
	súdne orgány

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.

SL	sodstvo
SV	dömande makt
	domarkår
	rättsväsen
	domstolsväsen

It is interesting to notice that the term has different interpretation and often there are more than one translation in the same language. This implies that from a linguistic perspective the term is quite ambiguous and include not only the physical person of the judge but the judicial system and in general the judicial power within a state.

1.2. The CJEU case law analysis by analogy

Reasoning by analogy, we could consider a situation similar to that under investigation to define a notion of judiciary in general terms applicable to all Member States. The Court of Justice of the European Union (CJEU) has pronounced itself on the issue of the reference for a preliminary ruling, which is to be exercised before the CJEU on the interpretation or validity of European law.

Article 267 of the Treaty on the Functioning of the European Union provides that the jurisdiction for preliminary ruling should be activated only by bodies, which correspond to the notion of jurisdiction of one of the Member States. It is therefore necessary to determine the parameters for a correct identification of this concept. The main difficulties encountered depend on the different organizational forms of the various legal systems of the Member States and on the different notions of jurisdiction found in each of them.

The Court, with the aim to overcome the particularities of each legal systems, has achieved, for reasons of uniformity, to the development of a "generic" notion of "jurisdiction" What it is relevant is 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.

substantially jurisdictional nature of the functions exercised by the body and not its *nomen iuris*, nor its classification in the national judicial system.

On the basis of EU law, this notion includes all bodies that fulfil the following requirements[7]: i) legal origin; ii) permanent nature, i. e. the circumstance that they do not exercise jurisdictional functions on an occasional basis; iii) mandatory nature of its jurisdiction; iv) contradictory nature of the proceeding; v) the fact that they apply juridical norms and do not pronounce according to equity; vi) autonomy and impartiality with respect to the parties to the proceedings. Only those proceedings relating to the exercise of administrative functions are excluded, even in the context of the judicial power (e.g. appointments), or those proceedings in which the referral body performs a function that is not purely jurisdictional, but merely a consultative one.

With this in mind, bodies of private origin or, in any case, emerged as an expression of professional autonomy[8] are excluded within the notion of judiciary. The arbitration boards[9] are also excluded from the aforementioned concept. The Court's attitude was different in the case of "almost" arbitration bodies operating in the social, professional or commercial sector, when they were established by law and invested with a mandatory competence[10]. In the case of public authorities, the Court ruled on the admissibility of the reference for a preliminary ruling but made a series of distinctions. If it considered the references for a preliminary ruling made by special boards of appeal in the field of public procurement[11] and by the Spanish competition authority[12] to be admissible, the references of the Greek competition authority[13] and the Austrian Telecommunications Control Commission were inadmissible[14]. Finally, it should be noted that the body that intends to carry out the reference for a

---

7 CJEU, 30.6.1966, Vaassen-Göbbels, *C-61/65*; 17.9.1997, Dorsch Consult, C-54/96 ;10.12.2009, Umweltanwalt von Kärnten , C-205/08; 14.6.2011, Miles, C-196/09

8 CJEU, order 18.6.1980, Borker, C-138/80; 19.9.2006, Wilson, C-506/04

9 CJEU, 23.3.1982, Nordsee, 102/81

10 CJEU, 17.10.1989, Danfoss, 109/88.

11 CJEU, 17.9.1997, Dorsch Consult, C-54/96; 14.11.2002, Felix Swoboda, C-411/00.

12 CJEU, 16.7.1992, Asociación Española de Banca Privada e a., C-67/91

13 CJEU, 31.5.2005, Syfait, C-53/03.

14 CJEU, order 18.6.1980, Borker, 138/80; 12.11.1998, Victoria Film, C-134/97; order 12.1.2010, Amiraike Berlin, C-497/08.

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.

preliminary ruling, should possess the quality of jurisdiction not only in the institutional sense of the term but also in the functional sense, that is to say that it must actually exercise, in a specific case, the function of judge and not that of an administrative authority.

This cognitive process of analogy could help to detect the specific requirements, which identify the role of judiciary.

1.3. Definition of the "judiciary" for INFORM project

The brief analysis envisaged helps to partially clarify the meaning of judiciary for the INFORM project purposes. The present Review Report needs to focus on a very practical approach to define the judicial target group for the analysis of the GDPR with respect to different categories of target groups within the INFORM project. The objective is to try to define a unique and neutral definition suitable for all Member States. The definition that is proposed must be operative and reduce the area of ambiguity. In such a context, under the INFORM project the judiciary is defined as:

The judicial authority as the complex of bodies fulfilling the roles of judges (individual judge or a panel of judges, professional judges or lay judges) and investigators (prosecutors, criminal investigation department).

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 2: Material scope of application of the GDPR with respect to judiciary: Art. 2

2.1 The context: the impact on the judicial system

Nowadays the need for uniform data protection standards is becoming increasingly high, due to the emerging of new challenges posed by the digital era. Data can easily cross borders and play a key role in global digital economy. The processing of personal data takes place in various spheres of economic and social activity, and the progress in information technology makes the processing and exchange of such data considerably easier[15]. In this context, the European Union (EU) adopted the General Data Protection Regulation (GDPR) to further harmonise the rules for data protection within the EU Member States and to raise the level of privacy for the affected individuals.

In particular, in the world of justice the relevance of data protection and privacy issue is increasingly recognized. The use of ICT technologies, on one hand, represents the key element to crucially improve the administration of justice and at the same time it opens up to relevant problems related to the data protection field.

The introduction of ICT had become essential to the efficient functioning of a judicial system, in pursuit of better access to justice, easier procedures in every branch of law (civil, criminal and administrative) and closer cooperation between different judicial authorities in EU countries. Furthermore, the availability of web services, the possibility of using electronic filing, the electronic exchange of legal documents, implementation of on-line proceedings can help judiciary to enhance and offer adequate services to the citizens and to give back efficiency, transparency and confidence to the administration of justice. In such a context, large amount of personal data is collected, processed and stored and many implications related to data protection issues rise with respect to judiciary when processing data in their daily activities and practices.

[15] Rec. 4 Data Protection 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.

Judiciary across Europe has to deal with a current highly fragmented system of data protection, with different national regulatory approaches, diverse procedures and practices in collecting, handling and storing personal data. Data processing activities that are allowed in one Member State could be illegal in another one with respect to a specific execution of personal data processing activity. Furthermore, national data protection laws provided different levels of protection which lead to legal uncertainty.

The first attempt to regulate data protection was the Directive 95/46/EC "on the protection of individuals with regard to the processing of personal data and on the free movement of such data". This legislative act set out the minimum standards on data protection in the whole of Europe to achieve an equivalent level of protection of the rights and freedoms of individuals with regard to the processing of such data, in all Member States. The aim of the Directive was to remove the divergences among national laws in the Member States so to ensure a consistent and uniform regulation of the flow of personal data. Each country within the EU has taken Directive 95/46/EC and transposed it into their own, national data protection laws.

In December 2015 the process of agreeing on a new set of legislation to reform the legal framework for ensuring the rights on data protection of EU citizens, was completed. This set of legislation was ratified in early 2016. It is called Regulation (EU) 2016/679, the General Data Protection Regulation (GDPR) and will replace national data protection laws, such as the ones mentioned above, being valid in every country of the EU. The principles of the Directive and the GDPR have the same background. In addition, the GDPR is intended to harmonize data protection law across the EU by removing the need for national implementation. On the 25th of May 2018, the 1995 Data Protection Directive will be replaced by the GDPR. One of the most significant changes in the GDPR is the very fact that it is a "regulation," as opposed to a "directive." The GDPR leaves a considerable margin for the EU Member States to enact national data protection legislation, both regarding the specification of the rules of the Regulation and sector-specific data protection.

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

Objectives

To further harmonise the rules for data protection within the EU Member States and to raise the level of protection for the affected individuals.

Impact on judicial system

In contrast to the Data Protection Directive, the Regulation directly applies to its addressees - little implementation measures by the EU Member States are required. By equalising the rules for data protection, the GDPR shall lead to more legal certainty and remove potential obstacles to the free flow of personal data. Judiciary as other project target groups will benefit from a consistent and uniform data protection framework.

2.2. Article 2 of the GDPR: material scope of application

The GDPR has a very wide scope of application, both materially and geographically. This paragraph offers information on the target group of Judiciary, subject to obligations under the GDPR by summarising the Regulation's material scope of application.

Article 2 governs the material scope of the GDPR. The GDPR retains much of the jargon from the Directive, although with some important changes.

The article states that "This Regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system".

For the judiciary is important to take into account the meaning of "processing" and "personal data": only having a clear knowledge of the activities and of the data that are covered by the Regulation, they should verify if their daily work falls within the scope of 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.

Processing

The Regulation has very broad material scope: it applies to any processing of personal data, in order to ensure and foster a high level of protection. According to Article 4, Sec. 2, the GDPR involves all processing activities regarding personal data, such as collecting, recording, organizing, structuring, adapting and altering, storing, retrieval, consulting, using, disclosing and erasing of data. It should be further noted that the listing of activities provided for in Article 4, para 2 of GDPR is not exhaustive. Thus, processing could also manifest itself capturing, scanning and processing the personal data contained in hard copy documents and even the simple fact of having access to them.

Moreover, the intention of the legislator of the GDPR is not to define specifically what the meaning of "processing" is: the use of an opening word in the text of Article 2 was intentional, in order to make the scope of application of the Regulation independent from technological developments.

Recital 15 of the GDPR explicitly establishes that "in order to prevent creating a serious risk of circumvention, the protection of natural persons should be technologically neutral and should not depend on the techniques used". Technological neutrality has been chosen as the goal of the new Regulation, since it is the only way to protect natural persons efficiently, regardless of the various technologies that might be used.

The objectives of technology neutral legislation should be to focus on the effects and not the means: there is no imposition of a particular technology, leaving the technological field open for development. To better underline these aims, the legislation firstly regulates the behaviour of persons and not of the machines. Afterwards, the legislation aims at regulating the use of the technology and not the technology itself. The examined legislation is concerned with the lawful processing of personal data and the protection of individuals' rights. Finally, any systematic handling of personal data independent from technological changes corresponds to the notion of "processing" under the material scope 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.

The notion includes processing carried out wholly or partly by automated means, (the latter meaning any processing where certain steps are carried out by individuals, such as entering data into a computer system), as well as "other than by automated means".

By definition, not only automated treatment, but also manual processing of personal data has been considered as processing under GDPR. In contrast to automatic processing through technology, manual processing is being entirely executed by humans without using tools or machines. By its very nature, this works much slower and less data can be processed. Therefore, manual processing only falls within the definition of "processing" under the GDPR if two conditions are being met:

- Such data need to form part of a filing system or intended to form part of that system (Art. 2, para. 1 GDPR). Based on predefined structure rules, a filing system divides data into different groups that are systematically managed;

- According to Recital 15 those files must be structured according to specific criteria. The Regulation does not specify any requirements for those specific criteria. Given prior legislation and the broad manner of interpretation of the GDPR, for example, chronically, alphabetically organised files, or files organised according to pre-determined categories should meet those conditions.

Personal data

The Regulation applies only to the processing of "personal data", which is defined in Article 4, Sec. 1, of the GDPR as "any information relating to an identified or identifiable natural person (a "data subject"). To be more specific, the Regulation applies to personal data of a natural living person. Recital 27 of the GDPR explicitly excludes the application of the new Regulation to the deceased persons. Moreover, legal entities do not benefit from protection under the GDPR, regardless of their legal form[16]. This is due to the fact that the legislator's will is wanted to enforce the protection of individuals with regard to their fundamental rights under Art. 8 of the Charter of Fundamental Rights of the

[16] Rec. 14 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.

European Union and Art. 16 of the Treaty on the Functioning of the European Union (TFEU)[17]. However, the data of legal persons could be deemed personal data under the GDPR if they contain information on the individuals associated with the legal person, e.g., information on a persons' share or function in a company.

Identifiability

Data is deemed personal not only if it belongs to an already identified individual, but also if the identification of a person is merely possible (identifiability). Identification is made possible by combining different information that by themselves would not have traced back to the person but does so in combination. The wording of Art. 4, sec. 1 does not state who needs to be able to identify the data subject, suggesting that the additional information does not necessarily have to be in possession of the data controller/processor.

Data is therefore personal if the identification of a person is possible based on the available data, meaning if a person can be detected, directly or indirectly, by reference to an identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person (Article 4, Sec. 1).

The definition is deliberately a very broad one in coherence with the other definitions provided for in the GDPR.

There are different ways in which an individual can be considered directly "identifiable" by reference to an identifier. In particular, the identifier should include:

- a person's name (the name of a person is the most common element that identifies directly an individual);
- an identification number (such as an ID number, a social security number, passport number, a

[17] Rec. 1 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.

car registration number, etc.);

- a location data or address;
- an online identifier (this may involve IP addresses or cookies). Recital 30 of the GDPR clarifies "online identifier" as below: "Natural 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".

In cases where the extent of the available identifiers does not allow anyone to select specifically and univocally an individual, that individual might still be identifiable due to the combination of such available information with other pieces of information. This is where the Regulation comes in with "one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person"

According to Recital 26 in order to affirm identifiability, the circumstances of the individual case have to be taken into account. This includes the following:

- the costs and time required for identification;
- the technology available at the time of the processing and technological developments;
- the purpose of the processing.

The requirement of taking into account technological developments might prove difficult in practice, as this means that data controllers/processors need to include foreseeable or likely technological developments in their decision-making processes. If the purpose of the processing can only be achieved upon knowledge of the data subjects' identity, it can be assumed that 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.

controller/processor has the means for identification. The faster and easier an individual can be made out, the more likely it is an 'identifiable individual'.

Key concepts

Processing.

DEFINITION: The GDPR applies to any processing of personal data. The (material) scope is interpreted in a very broad manner in order to ensure a high level of protection. It includes any processing activities such as collecting, recording, organizing, structuring, adapting and altering, storing, retrieval, consulting, using, disclosing and erasing of data.

Treatments carried out "wholly or partly by automated means" as well as "other than by automated means":

DEFINITION: Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means

In case of manual processing, two conditions need to be met: a) personal data need to form part of a filing system or intended to form part of that system; b) files or sets of files, as well as their cover page" have to be structured according to specific criteria.

Personal data:

DEFINITION: Any information relating to an identified or identifiable living natural person (a "data subject").

The GDPR does not apply to deceased persons and to information of legal persons (Recital 27 and Recital 14).

Identified or identifiable natural person:

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.

DEFINITION: A) Identified: a person who, within a group of persons, can be distinguished from all other members of the group. B) Identifiable: natural living person, who is a person who can be identified, directly or indirectly, by reference to an identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Keep in mind for judiciary

Judiciary should have an in-depth and accurate knowledge of the meaning of the terms and concepts provided in Article 4, Sec. 1 of GDPR. When processing personal data, judiciary should be aware to make their activities in a lawful manner as to be compliant with the new data protection Regulation. This is the only one way for judiciary to ensure a proper respect of data protection rules and to reach a consistent and uniform application of the Regulation and, meanwhile, an appropriate level of protection for data subject's rights.

2.3 Exemptions from the material scope of the application of the GDPR

Article 2, Sec. 2 of the GDPR provides for in four exemptions from the scope of application of the new data protection legislation.

The GDPR does not apply:

- *Lit a): to the processing of personal data in respect of activities which fall outside the scope of EU law*. In particular, Recital 16 of the GDPR specifies that these activities should concern national security.

- *Lit b): to the processing of personal data by Member States when carrying out activities which fall within the scope of Chapter 2 of Title 5 of TUE*. Recital 16 of GDPR specifies that the activities are those in relation to the common foreign and security policy of the Union.

- *Lit c): to the processing of personal data by an individual in the course of a purely personal or household activity*.

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.

According to Recital 18 of GDPR those activities could include the processing of data for leisure activities, hobbies, vacation or entertainment purposes, or for the use of social network. This notion should be interpreted based on the general social opinion and includes personal data that is being processed for the use of a social network or data that is part of a personal collection of addresses, birthdays or other important dates, such as anniversaries. From practical point of view, GDPR does not apply to issues arising from private citizen's processing of personal data, when the processing is limited to their own individual or household activities. According to Recital 18 it should be noted that if processing concerns both private and business information, the exception will not be applicable. The word "purely" implies such *narrow interpretation* of this exception. It is important to have clear knowledge whether the processing falls within the exemption or not. A set of criteria developed under the Directive 95/46/EC interpretation were implemented to determine as objectively as possible the boarders of this exemption. Those criteria, just to give some examples, refer to:

1. The dissemination of personal to an indefinite number of persons rather than a limited community of friends, family members.

2. The scale and frequency of the processing of personal data (that could hide professional or commercial activity).

The future data protection approach to the processing of personal data done for personal or household purposes, which will be established under the entrance into force of the GDPR, will be opened to interpretation and specification and, probably, further detailed criteria will be developed.

- *Lit d): to the processing of personal data for criminal persecution*. More specifically, 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, including the safeguarding against and the prevention of threats to public security" does not fall within the scope of the Regulation. This latter exemption is the most important one from a legal point

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 view, and judiciary has to consider this exclusion from the scope of application of the GDPR as to adapt their activities, when processing personal data, to 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[18]. **Key concepts**

1. Processing of personal data in respect of activities which fall outside the scope of EU law (for example national security)

2. Processing of personal data by Member States when carrying out activities which fall within the scope of Chapter 2 of Title 5 of TUE (such as common foreign and security policy of the Union)

3. Processing of personal data by an individual in the course of a purely personal or household activity

Judiciary has to bear in mind this exclusion from the scope of application of data protection legislation when processing personal data. In those cases, judiciary should interpret the notion "purely personal or household activity" in a narrow manner, using objective and fair criteria. Moreover, judiciary has to consider carefully the developments done in the interpretation/elaboration of such criteria.

4. Processing of personal data for criminal persecution by competent authorities

[18] Please note that D2.2 developed under INFORM provides an overview of the Directive in view of its application by the judiciary.

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.

Application of Directive 2016/680/EU. When judiciary acts as "competent authority" within the meaning of Directive 2016/680/EU and for criminal persecution, its activities on personal data processing fall under the Directive regime.

Keep in mind for judiciary

Judiciary has to consider those exclusions from the scope of application of data protection legislation as to adapt its activities, when processing personal data, to the specific legislation issued at EU and/or national level.

2.4. Specific Member States and EU legislations in the field of personal data processing activity

Recital 19 specifies that personal data processed by public authorities under the GDPR regime, when used for criminal persecution purposes, should be regulated by the Directive 2016/680/EU. If personal data is processed for other purposes by those competent authorities within the meaning of Directive 2016/680/EU in so far as the processing falls under the scope of Union law, the GDPR should be applied. Even if the GDPR does not require any implementing measures into the national law of the EU Member States, it provides for different opening clauses that explicitly allow each Member State to issue national legislation. Recital 19, second part, of the GDPR, with regard to the processing of personal data by those competent authorities for purposes falling within the scope of the Regulation, expressly establish that each Member State might preserve or bring in peculiar provisions to adapt the application of the rules of this Regulation to specific areas of data protection. In those cases, judiciary (who might act as "competent authority" within the meaning of Directive 2016/680/EU) has to consider carefully national peculiarities and, when implementing its data processing activities, judiciary has to take into consideration if specific rules concerning data protection are introduced by Member States, if expressly allowed by the new Regulation. To be more precise, judiciary has to examine on a case to case basis whether national legislation of EU Member States

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.

introduces or maintains national provisions that may determine more precisely specific requirements for the processing of personal data.

Furthermore, Recital 20 of the GDPR provides a specific provision for courts and other judicial authorities and allows EU Member States to introduce specific provisions in the field of personal data processing activities.

While Recital 20 clarifies that the GDPR applies*, inter alia,* to the activities of courts and other judicial authorities, nevertheless it specifies that Union Member State laws could further state the processing operations and processing procedures regarding the treatments of personal data conducted by those courts and judicial authorities.

What is important to underline in Recital 20 is the provision that ensures the independence of the judiciary in the performance of its judicial tasks, including decision-making. Recital 20 states that the competence of the supervisory authorities should not cover the processing of personal data when courts are acting in their judicial capacity. Supervisory Authorities as "independent public authorities" established at national level (Article 4, Sec. 21 of the GDPR), will continue to exist. But, because of the independence of judiciary, of its specific legal qualifications, experience and skills as well as of its autonomy as one of the three pillars of the State, the control of those national supervisory authorities does not cover the personal data processing activities when judiciary exercises its function/role.

Finally, after introducing specific exemptions from the material scope of the application of the GDPR, Art. 2, Para. 3 and Para. 4 establish the application of other EU legal acts to the personal data processing activities:

- Regulation (EC) No 45/2001 of the European Parliament and of the Council applies to the processing of personal data by the Union institutions, bodies, offices and agencies, in so far as its provisions be adapted to the principles and rules established in the new data protection Regulation and apply in the light of GDPR.

- Directive 2000/31/EC on certain legal aspects of information society services, in particular

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.

electronic commerce, in the Internal Market ("Directive on electronic commerce"). The Directive aims at contributing to the correct functioning of the internal market by removing obstacles to cross-border online services (free movement of services). In particular, liability rules of intermediary service providers will continue to be applicable.

Key concepts

Processing of personal data for other purposes by competent authorities within the meaning of Directive 2016/680

GDPR does apply, as long as the processing falls under the scope of Union law.

Member States should be able to maintain or introduce more specific provisions to adapt the application of the rules of this Regulation.

Personal data processing activities of courts and other judicial authorities

GDPR does apply.

Member State law could specify the processing operations and processing procedures in relation to the processing of personal data by courts and other judicial authorities.

Keep in mind for judiciary

Judiciary has to keep track on how the open clauses are transposed into national legislation. Therefore, it will be essential for judiciary to review its data protection practices and procedures not only in line with GDPR requirements, but also in line with national provisions, which are issued explicitly in order to adapt the application of the rules of the new Regulation.

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: Data type and data processing activities performed by judiciary

3.1. Who is data controller and who is data processor?

The GDPR and its principles provide the conditions on which an entity is permitted to process personal data. If an entity cannot satisfy these principles (and if no exemption or derogation applies) then such processing will be unlawful. As a consequence, it is of paramount importance for entities to know and understand these principles and to examine the risks related to the processing of personal data activities. To face and reduce these risk, the EU legislator has established a series of obligations for the entities carrying out personal data processing activities

Data processing activities of judiciary should be performed in compliance with the principles of GDPR, guaranteeing that:

- the rights of individuals with regard of the processing of personal data, are protected;
- the personal data processing activities have been carried out lawfully.

In this context, judiciary plays a key role as it represents across EU countries one of the three pillars of the State: it performs its duties out of influence or control of the other actors, whether public or private entities. What is important to take into account, when data protection issues arising, is that those issues are not obstacles to an efficient administration of justice. Data protection legislation could for example influence or modify the collection and processing of enormous amount of information, helping in preventing massive reproduction of data, increasing data quality, or reducing security risks.

3.1.1 The notion

Every time an entity processes personal data, it will do so as either a controller or a processor. These roles bear different responsibilities. Therefore, it is crucially important for an entity to be able 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.

- identify the scenarios in which it acts as a controller and/or processor;
- understand the obligations that apply to controllers and/or processor;
- comply with those obligations.

Judiciary is subject to obligations under the GDPR, depending on whether or not it should consider as a data controller and/or a data processor.

What judiciary should keep in mind is that the most relevant consequence of being a data controller or a data processor is legal responsibility/accountability for complying with the obligations under the GDPR.

3.1.2 Determination based on the definition in Art. 4, sec. 7 and 8

GDPR introduces an essential change respect to the previous data protection legislation: both data controllers and data processors will be jointly and individually responsible for compliance within the new Regulation. These roles have different degree of accountability.

It is vital for judiciary that acts as data controller or data processor to:

- identify if a subject acts as a controller or processor;
- understand its responsibilities as a controller or processor;
- review all of its data processing activities in preparation for the GDPR;
- identify the data processing activities for which the judiciary is a controller or a processor, and ensure that it understands its responsibilities as a controller;
- ensure that, in respect of each processing activity for which it is a controller, it has implemented appropriate technical and organizational measures to ensure compliance with the GDPR. Art. 24 of the GDPR explicitly states that "the controller is responsible for implementing appropriate technical and organizational measures to ensure and to demonstrate that its

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 activities are compliant with the requirements of the GDPR". Examples of such measures can be the distribution of responsibilities for data protection, a data protection impact assessment and a risk mitigation plan, implementation of pseudonymisation and data minimization in order to meet the specific GDPR requirements and protect the data protection rights of data subjects.

Data controller

Art. 4, sec. 7 of GDPR defines the data controller as "the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data". The concept of a controller is essentially unchanged under the GDPR. Any entity that is a controller under the Directive likely continues to be a controller under the GDPR.

The GDPR does not provide specific criteria to identify a data controller. Nevertheless, some relevant parameters have been elaborated under the previous data protection legislation, to determine whether a subject should be considered as a data controller[19].Judiciary that acts as a controller should decide:

- to collect the personal data in the first place and which is the legal basis for doing so;
- which items of personal data to collect, such as the content of the data;
- the purpose or purposes the data are to be used for;
- which individuals to collect data about;
- whether to disclose the data, and if so, who to;

[19] If more than one entity is entitled, in relation to any processing activity to be the controller (on the basis that more than one entity may make decisions about the purposes for which, and means by which, those data are processed) a joint controllership scenario arises. Where liability arises in a joint controllership scenario, the issue of how liability should be distributed between the joint "data controllers" is not a fundamental question from the perspective of the GDPR. The main focus is the best protection for data subject's rights. The GDPR makes joint controllers fully liable. Once "full compensation" has been paid to the affected data subject, joint controllers may recover damages from one another.

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 subject access and other individuals' rights apply;
- how long to retain the data or whether to make non-routine amendments to the data.

Considering the given meaning of data controller and taking into consideration the independence that characterizes judiciary functions, it can be assumed that judiciary generally acts as a data controller. As data controller, judiciary should exercise an overall control over the purposes for which, and the way, personal data are processed. Only having a clear understanding and knowledge of its role as data controller, judiciary should guarantee compliance with the GDPR and should foster and ensure a better safeguard of citizen's data protection rights in the judicial system.

Data processor

Art. 4, sec. 8 of the GDPR identifies the data processor as "a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller". The GDPR identifies the data processor with the entity who is delegated to implement the instructions given by the data controller. The lawfulness of the data processing activities carried out by the data processor depends on such delegation. The data controller could decide either to process personal data on its behalf, or to delegate specific task/activities related to the processing of personal data to an external body.

Two conditions should be met:

- The data processor should be a separate legal entity with respect to the data controller;
- The data processor should process personal data on behalf of the data controller.

The relationship between the controller and processor is based on the principle that the processor will only process data in accordance with the controller's instructions. Processors shall not process personal data, except in accordance with the instructions of the controller, or the requirements of EU law or the national laws of Member States (Art. 29 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.

Under the GDPR, the concept of a processor does not change. Any entity that is a processor under the Directive would likely continue to be a processor under the GDPR. However, whereas the Directive generally only imposes direct compliance obligations on controllers, the GDPR imposes direct compliance obligations on both controllers and processors, and both will face direct enforcement and serious penalties if they do not comply with the GDPR.

Where a processor, in breach of the GDPR, determines the purposes and means of any processing activity (i.e., if the processor makes its own decisions, rather than following the controller's instructions), that processor is treated as a controller in respect of that processing activity (Art. 28, Para. 10). Furthermore, in specific situations, the data processor, besides processing personal data for others, should be considered as a data controller. The data processor may act as a data controller when certain processing activities on personal data are carried out for its own purposes.

Key concepts

Data controller

The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data (Art. 4, sec. 7 GDPR)

Data processor

The natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller (Art. 4, sec. 2 GDPR)

Keep in mind for judiciary

Judiciary seems to work mainly as data controller in circumstances where it determines the purpose for which and the manner any personal data is processed. This is so in relation to data processed in the exercise of any judicial functions

Judiciary that acts as data controller should:

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.

- Identify the data processing activities for which it is a controller;
- Ensure that it understands its responsibilities as a controller under the GDPR; and
- Ensure that it has appropriate processes and templates in place for identifying, reviewing and (to the extent required) promptly reporting data breaches to the relevant controller.

3.2. The requirements of personal data and its limits

3.2.1 Pseudonomysation and anonymisation, Art. 4, sec. 5

Anonymisation and pseudonymisation represent two terms that have been the topic of much discussion since the introduction of GDPR. In general terms, anonymisation and pseudonymisation are two distinct techniques that permit data controllers and processors to use de-identified data. The difference between the two techniques is on whether the data can be re-identified. On the basis of Recital 26 of the GDPR anonymised data is "data rendered anonymous in such a way that the data subject is not or no longer identifiable." This definition highlights that anonymised data must be deprived of any identifiable information, making it impossible to derive insights on an individual, even by the party that is responsible for the anonymisation. According to the Article 29 Working Party true data anonymisation is an extremely high obstacle, and often data controllers are not able to actually anonymise data.

Judiciary has to take into consideration, when processing personal data, how the anonymisation and pseudonymisation procedures may be important aspects to GDPR compliance. Judiciary has to reach deep awareness of the existence of such techniques which can render data no-identifiable. At the same time, judiciary should analyse the effectiveness and limits of existing anonymisation and pseudonymisation techniques of data protection, at EU level, and has to carried out a cautious and responsible use of these techniques to ensure a well-building system of protection of data subject's rights.

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.

Judiciary should take into account that:

- Anonymisation of data can be a good strategy to 'release' such data from the legislative regime;
- pseudonymisation should be a de-identification technique that ensure some level of flexibility under the GDPR, even though the data will still be considered to be personal data and fall under the scope of application of EU data protection law.

Judiciary should pay special attention to the potential residual risk related to re-identification of data and its potential impact on data protection rights. Anonymisation and pseudonymisation can provide data protection guarantees and might be used to achieve efficient processing of data as well as compliant with the applicable legislation.

Anonymisation

Data are anonymised if all identifying elements have been removed from a set of personal data. Any information which could serve to re-identify the person should have been eliminated. Therefore, data that are fully anonymised (i.e., data from which no individuals can be identified) are outside the scope of the GDPR.

As previously mentioned Recital 26 specifically defines anonymised data, as "data rendered anonymous in such a way that the data subject is not, or no longer, identifiable." The aim of anonymisation technique is to irreversibly prevent identification of the data subject. In other words, anonymisation technique should avoid that anonymised personal data could be re-identified.

If the data controller retains the raw data or any other information which can be used to reverse the anonymisation process and to identify a data subject, the identification by the data controller must still be considered possible in most cases. Therefore, the anonymised data must normally still be considered personal data and should only be processed in accordance with the GDPR. Where data has been anonymised to such an extent that it would not be possible to identify an individual in the anonymised

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 even with the aid of the original data, the anonymised data is not considered personal data. Several anonymisation techniques may be envisaged, but generally those techniques fall within two categories:

- Randomisation: this technique alters the veracity of the data in order to remove the strong link between the data and the individual. It should be combined with generalisation techniques to provide stronger privacy guarantees;

- Generalisation: it consists of generalising or diluting, the attributes of data subjects by modifying the respective scale or order of magnitude (for example a region rather than a city, a month rather than a week).

Pseudonymisation

Pseudonymous data represents data that can be amended in such a way that no individuals can be identified from this data (whether directly or indirectly) without a "key" that allows the data to be re-identified. Article 4, sec. 5 of the GDPR defines pseudonymisation as "the processing of personal data in such a way that the data can no longer be attributed to a specific data subject without the use of additional information". Pseudonymisation substitutes the identity of the data subject in such a way that additional information is required to re-identify the data subject. With respect to anonymisation, the risk of re-identification is higher.

Pseudonymous data is still treated as personal data because it enables the identification of individuals. However, provided that the "key" that enables re-identification of individuals is kept separate and secure, the risks associated with pseudonymous data are likely to be lower, and so the levels of protection required for those data are likely to be lower.

Differently from anonymisation technique, pseudonymisation does not exempt data from the scope of the GDPR. While personal data is most definitely the class of information covered by the GDPR and anonymised data is not regulated by definition, pseudonymised data represents a useful compromise position. It allows a data controller to afford some protection over the data, by, for example, minimising the chances that the underlying identities will be revealed.

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.

Indeed, Recital 26 states that "data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information, should be considered to be information on an identifiable natural person".

The GDPR explicitly encourages data controller to consider pseudonymisation as a security measure. In fact, pseudonymisation of data provides advantages. It can allow entities to satisfy their obligations of privacy by design and privacy by default and it may be used to justify processing that would otherwise be deemed "incompatible" with the purposes for which the data were originally collected.

Key concepts

Anonymisation

The technique by which data has been rendered anonymous in such a way that the data subject is not, or no longer, identifiable

Pseudonymisation

The technique by which the processing of personal data is carried out in such a way that the data can no longer be attributed to a specific data subject without the use of additional information.

Keep in mind for judiciary

Judiciary has to analyse the effectiveness and limits of existing anonymisation and pseudonymisation techniques of data protection, at EU level, and has to carry out a cautious and responsible use of these techniques to ensure a well-building system of protection of data subject's rights.

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.

3.2.2 Special type of data and the consequences for data processing, Art. 9

3.2.2.1 Introduction

The GDPR provides elevated protection for special types of personal data, by expressly prohibiting its processing, unless specific conditions apply.

Pursuant to Art. 9, para. 1 of the GDPR, the following types of sensitive personal data revealing[20]:

- racial or ethnic origin;
- political, religious, or philosophical beliefs, including trade-union membership;
- data concerning health, sex life, and sexual orientation;
- genetic and biometric data (for the purpose of uniquely identifying an individual,

may not be processed.

Due to the high level of sensitivity, data relating to criminal offences and convictions is addressed separately[21]. Art. 9, Para. 2 of the GDPR specifically introduces exceptional situations of processing sensitive personal data. The list below should be considered exhaustive:

- explicit consent of the data subject;
- employment and social security;
- vital interest;
- membership organisation;
- publicly disclosed data;

[20] **The term** "revealing" is to be understood in this meaning: not only data which by its very nature contains sensitive information is covered by this provision, but also data from which sensitive information, with regard to a natural person, can be deduced.

[21] Criminal convictions might mark out the natural person concerned, thus Art. 10 of GDPR does not provide exceptional situations of processing those sensitive data that permit entities to deviate from the stronger requirements in art. 10 itself. More specifically, processing of personal data relating to criminal convictions and offences or related security measures, based on a legal permission under art. 6 section 1 of the GDPR (for example, consent, contractual necessity of processing, prevailing legitimate interest of the controller, etc.) shall be carried out only if one of the following requirement is being met: a) processing is under the control of official authority; b) the processing is authorized by Union or Member State law, providing for appropriate safeguards for the rights and freedoms of data subjects.

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.

- legal proceedings;
- substantial public interest;
- medicine;
- public health;
- research purposes.

It is extremely important for judiciary to understand the different levels of protection set out in the GDPR for personal sensitive data. Those data should allow conclusions, and in specific cases stigmatisation (see criminal convictions), about an individual that are strictly linked to his/her fundamental rights and freedoms and their processing might entail high risks for the individual. Moreover, information about those special types of personal data could be used in an unlawful and discriminatory way.

If judiciary is processing sensitive personal data, one or more of the conditions provided in Art. 9, Para. 2 has to be satisfied, as well as one of the general conditions which apply in every case (see Art. 6 of the GDPR, "Lawfulness of processing"). In other words, when processing sensitive personal data, judiciary needs to identify different conditions, that do not have to be linked[22]:

- A lawful basis for processing under Art. 6, in exactly the same way as for any other personal data.

- A specific condition under Article 9, Para. 2 of the GDPR.

22: "Your choice of lawful basis under Article 6 does not dictate which special category condition you must apply, and vice versa. For example, if you use consent as your lawful basis, you are not restricted to using explicit consent for special category processing under Article 9. You should choose whichever special category condition is the most appropriate in the circumstances – although in many cases there may well be an obvious link between the two. For example, if your lawful basis is vital interests, it is highly likely that the Article 9 condition for vital interests will also be appropriate".

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.

3.2.2.2 Sensitive personal data: the different categories

As above mentioned, Art. 9, Para. 1 of the GDPR introduces a conclusive list of sensitive personal data, distinct from all other personal data. The special characteristic of those data is the requirement of extra protection and the processing by the data controller only under specific conditions. Below a brief description of the specific personal sensitive data set out in Art. 9 of the GDPR:

- **Data revealing racial or ethnic origin**

This category is particularly sensitive as it might lead to a discrimination of a natural person. Recital 51 specifically points out that the use of the term "racial origin" in this Regulation does not imply an acceptance by the Union of theories, which attempt to determine the existence of separate human races. For example, these data should be considered as ethnic/racial markers such as a person's country of origin, place of birth of parents, the native language, etc.

- **Data revealing political opinions**

This category should include information on a natural person's membership in a political party, on a participation in a political reunion or similar event, as well as on the support of a certain political trend. In particular, Recital 56 establishes that, "where in the course of electoral activities, the operation of the democratic system in a Member State requires that political parties compile personal data on people's political opinions, the processing of such data may be permitted for reasons of public interest, provided that appropriate safeguards are established".

- **Data revealing religious or philosophical beliefs**

This category merits specific protection since the processing of such data could lead to a discrimination of individual, in order to safeguard the risk to the rights and freedoms of natural persons when practicing religion.

- **Data revealing trade union membership**

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.

This category relates to information on individuals trade union activities and should be used in a discriminatory way in the employment market.

- **Data concerning health**

Art. 4, sec. 15 of the GDPR refers to data concerning health, which 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/ her health status.

More specifically, Recital 35 of the GDPR establishes that personal data concerning health should include all data pertaining to the health status of a data subject which reveal information relating to the past, current or future physical or mental health status of the data subject. This should include information about the natural person collected in the course of the registration for, or the provision of, health care services to that natural person. Moreover, data concerning health should be considered a number, symbol or particular assigned to a natural person to uniquely identify the natural person for health purposes; information derived from the testing or examination of a body part or bodily substance, including from genetic data and biological samples; and any information on a disease, disability, disease risk, medical history, clinical treatment or the physiological or biomedical state of the data subject independent of its source, for example from a physician or other health professional, a hospital, a medical device or an in vitro diagnostic test.

From a judicial perspective, health data should be relevant when dealing with insurance litigation, personal injury lawsuit (claims for medical expense reimbursement, claim damages for lost wages or diminished employment opportunities), as well as in case of criminal investigation (for instance expert reports on health condition of an individual to be used in trial as evidence). It is to be noticed that Art. 9, Para. 4 of GDPR authorised Member States to maintain or introduce further conditions, including limitations, with regard to the processing of data concerning health.

- **Data concerning an individual's sex life or sexual orientation**

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.

This category is deemed particularly sensitive as it should include information on gender identity, sex characteristics disclosing that the citizen has changed his/her name and the sex ascribed at birth.

- **Genetic and biometric data**

Genetic and biometric data was not explicitly provided for as protected categories under the former Directive 95/46/EC, but now it has been included under the scope of Art. 9, Para. 1 of the GDPR. Moreover, Art. 4, sec. 13 describes genetic data as 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.

In view of biometrics data, Art. 4, sec. 14 introduces biometric data as personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allows or confirms the unique identification of that natural person, such as facial images or dactyloscopic data.

For example, facial images or fingerprints are covered by the definition of biometric data. It is worth to note that Recital 51 of the GDPR suggests that the processing of photographs will not automatically be considered as sensitive data processing (as has been the case in some Member States to date); photographs will be covered only to the extent they allow the unique identification or authentication of an individual as a biometric (such as when used as part of an electronic passport). Both these categories of sensitive data are based on the same requirement: they should allow or confirm the unique identification of the natural person.

Judiciary ought to be aware that the misuse of sensitive data might be irreversible and have long-term consequences as well as strong impact for the natural persons. For this reason, the processing of such data has to be conducted by the judiciary depending on certain safeguards and conditions and paying specific attention.

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.

3.2.2.3 Exception from the prohibition of processing sensitive data

Art. 9, Para. 2 of the GDPR introduces several exemptions to the prohibition of processing sensitive personal data:

- **Explicit consent of the data subject (Art. 9, Para 2 lit. a)**

The prohibition of processing sensitive personal data does not apply when the data subject has given explicit consent to the processing of those personal data for one or more specified purposes. Such condition has to fulfil two requirements: on one hand, it has to respect the general provision for valid consent under Art. 7 of the GDPR; on the other hand, it has to explicitly refer to the processing of special categories of data.

There is only one exception to the processing of sensitive personal data, when Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject explicit consent.

- **Employment and social security (Art. 9, Para. 2, lit. b)**

This exception takes into account that the processing of sensitive data in the employment relationship is necessary, so that the data controller or the data subject can comply with employment law. In other words, the processing of such sensitive data is necessary for the purposes of carrying out the obligations and of exercising specific rights of the data controller or of the data subject in the field of employment, social security and social protection law.

In this case, the processing should be carried out, in so far as:

- it is authorized by Union or Member State law or by a collective agreement pursuant to Member State law,
- appropriate safeguards for the fundamental rights and the interests of the data subject are provided.

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.

- **Vital interest (Art. 9, Para. 2, lit. c)**

The processing of personal sensitive data is necessary to protect the vital interests of the data subject or of another natural person, where the data subject is physically or legally incapable of giving consent.

- **Membership organisation (Art. 9, Para. 2, lit. d)**

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

Two requirements are needed for processing sensitive personal data in such a context:

  - the processing is limited within members of the non-profit entity or persons that are regularly in contact with that entity.
  - sensitive personal data can be disclosed outside that body solely with the data subject's explicit consent.

- **Publicly disclosed data (Art. 9, Para. 2, lit. e)**

Processing relates to personal data which are manifestly made public by the data subject himself/ herself.

Naturally, this framework should refer to personal data entered in public registers, lists, acts or documents accessible to everyone, without a user account.

- **Legal proceedings (Art. 9, Para. 2, lit f)**

Processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity.

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.

This is the most important exemption for judiciary: for instance, the processing of sensitive data should be carried out for purposes of proof in the course of legal proceedings, to admit evidence in trial.

- **Substantial public interest (Art. 9, Para. 2, lit g)**

The processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law. Such legislation should be proportionate to the aim pursued, it should respect the essence of the right to data protection and it should provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

- **Medicine (Art. 9, Para. 2, lit h)**

The processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional.

Art. 9, Para. 3 specifically refers to further safeguard conditions in case the processing of those data is necessary for individual health care purposes on the basis of such contract. The sensitive data should be processed by or under the responsibility of a:

  - professional subject, who is obliged to the professional secrecy under Union or Member State law or rules established by national competent bodies.
  - another person also subject to an obligation of secrecy under Union or Member State law or rules established by national competent bodies.

- **Public health (Art. 9, Para. 2, lit i)**

The processing of sensitive data is necessary for reasons of public interest in the area of public health. According to Recital 54 of the GDPR, "public health" means health status, including morbidity and disability, the determinants having an effect on that health status, health care needs, resources allocated to health care, the provision of, and universal access to, health care as well as health care expenditure

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.

and financing, and the causes of mortality. Such exemption should also concern the protection against serious cross-border threats to health or the attempt to ensure high standards of quality and safety of health care and of medicinal products or medical devices. Moreover, the processing should take place on the basis of Union or Member State law, which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy.

- **Research purposes (Art. 9, Para. 2, lit j)**

The processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes based on Union or Member State law. Such legislation should be proportionate to the aim pursued, should respect the essence of the right to data protection and should provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

Key concept

Keep in mind for judiciary

Judiciary ought to be aware that the misuse of sensitive data might be irreversible and have long-term consequences as well as strong impact for the natural persons. For this reason, the processing of such data has to be conducted by the judiciary depending on certain safeguards and conditions and paying specific attention.

If judiciary is processing sensitive personal data, one or more of the conditions provided in Art. 9, para. 2 must be satisfied, as well as one of the general conditions, which apply in every case (see Art. 6 of the GDPR, "Lawfulness of processing").

3.3. Activities of data processing, Art. 4, sec. 2

According to Art. 4, sec. 2 of the GDPR, processing means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such

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.

as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

The GDPR contains a number of new protections for EU data subjects and threatens significant fines and penalties for non-compliant data controllers. Therefore, it is of the utmost importance for judiciary to have an in-depth knowledge regarding the operations, which can be conducted on personal data.

3.3.1 Collection[23]

This is the first stage of the cycle of data processing activities, and it is very crucial, since the quality of data collected will impact heavily on the output. The collection process needs to ensure that the data gathered is both defined and accurate, so that subsequent decisions based on this data are valid. Article 5 of the GDPR explicitly authorises associations and other bodies representing categories of controllers or processors to prepare codes of conduct or amend or extend such codes. The collection of personal data occurs in many cases: during the investigative phase and within the process about parties of the proceedings, about the suspect of a crime, about the witnesses, just for giving some examples. The data collection might be particularly relevant in case of gathering physical items that contain potential evidence (such as fingerprints, DNA, voice interceptions, etc.).

3.3.2 Recording and storage[24]

Having trace of processing activities is considered very important in the GDPR discipline. A lot of data is collected as part of judiciary daily activities, and it is of paramount importance to maintain a

23 Collection of fingerprints records: Eur. Court of HR, M.K. v. France, judgment of 18 April 2013, application no. 19522/09. Collection of health data: Eur. Court of HR, L.H. v Latvia, judgment of 29 April 2014, application no. 52019/07; Eur. Court of HR, Case of Zaichenko v. Ukraine, judgment of 26 February 2015, application no. 45797/09.

24 Storage of certain information about them in Security Police files: Eur. Court of HR, Segerstedt-Wiberg and Others v. Sweden, judgment of 6 June 2006, application no 62332/00. Storage in the context of criminal justice: Eur. Court of HR, Perry v. United Kingdom, judgment of 17 July 2003, application no. 63737/00; Eur. Court of HR, Peruzzo and Martens v. Germany, judgment of 4 June 2013, Applications nos. 7841/08 and 57900/12; Eur. Court of HR, Da Gregorio and Mosconi v. France, judgment of 8 November 2016, application no. 65714/11; Eur. Court of HR, Figueiredo Teixeira v. Andorra, judgment 8 November 2016, application no. 72384/14. Storage in the context of health: Eur. Court of HR, L.L. v. France, judgment 10 October 2006, application no. 7508/02. Storage in secret registers: Eur. Court of HR, Leander v. Sweden, judgment 23 March 1987, application no. 9248/81.

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.

record of processing activities in order to ensure the lawfulness of the processing and the protection of the data subject's rights and freedoms. The GDPR strengthens the importance of maintaining a record of the data processing activities performed by data controllers. According to Article 30 of the GDPR, the data controllers (and data processors) have to implement records of their processing activities that should permit (if validly maintained) to prove compliant with the GDPR. This provision should apply to judiciary in order to have a valid chain of data processing activities.

Storage is one of the latest stages in the data processing cycle, where data is held for future use. This step allows quick access and retrieval of the processed information. Judiciary has to pay strong attention to the storage of certain kinds of data. Due to the relevance of the data processed (see for example proceedings for child sexual abuse), storage activity should be organised with limited and authorized access in order to ensure secure data protection and, at the same time, to protect data controller's rights.

Personal data should be kept in a form that permits identification of data subjects for no longer than necessary for the processing purposes, according to Art. 5, para. 1 lit. e GDPR. This provision is substantiated by the controller's obligation to erase personal data under Art. 17 GDPR.

3.3.3 Organization and structuring

The abundance of digital information that today each data controller has to manage, implies that providing useful and usable tools to organize and handle this complexity is more important than ever. Judiciary has to daily face with an enormous amount of personal data: the more organised and structured data are, the better is their management in terms of data protection.

3.3.4 Adaptation or alteration

Those activities encompass all personal data processing activities that might modify or manipulate data collected. Those activities mainly take place when the data subject exercise the right of rectification.

3.3.5 Retrieval or consultation

The process of retrieval consists in the activity of extrapolation of data from already memorized categories of 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.

Consultation is the mere reading of personal data. Even the mere visualization of data is a treatment that can be included in the consultation operation.

3.3.6 Use, alignment or combination

The use is a generic activity that covers any type of data use.

The alignment is a comparison between data, as a consequence of processing, selection or consultation.

The combination consists of the use and interconnection of multiple databases, and refers to the use of electronic tools.

3.3.7 Disclosure by transmission[25]

It consists in giving knowledge of personal data to one or more specific subjects other than the interested party.

Recital 88 of GDPR establishes that it should have been taken into account the legitimate interests of law-enforcement authorities where early disclosure could unnecessarily hamper the investigation of the circumstances of a personal data breach.

According to recital 83 of GDPR in assessing data security risk, consideration should be given to the risks related to the disclosure of, or access to, personal data transmitted, stored or otherwise processed which may in particular lead to physical, material or non-material damage.

In other words, this processing activity is strictly related to personal data breach in case of unauthorized disclosure of personal data transmitted, stored or otherwise processed.

3.3.8 Dissemination or otherwise making available

This processing activity concerns the release of data to end users. It is the process of making personal data known to the public at large and/or to an indefinite amount of entities – for instance, by

25 Disclosure of personal data: Eur. Court of HR, Z. v. Finland, judgment of 25 February 1997, application no. 22009/97; Eur. Court of HR, Panteleyenko v. Ukraine, judgment of 29 June 2006, application no. 11901/02; Eur. Court of HR, Avilkina and Others v. Russia, judgment of 6 June 2013, application no.1585/09; Eur. Court of HR,

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.

publishing personal data in a daily or posting personal data on a web page.

From the perspective of the judiciary, it has to be considered that during the investigative phase, information should be communicated only to entities (police, public prosecutor) which are involved in the proceedings.

The dissemination process mainly concerns the online publication of judgments by judges.

3.3.9 Restriction

Special categories of personal data (sensitive data, such data on health, on sexual orientation or related to religious belief) could be ensured with higher level of protection, thus a restricted regime of access or use may be established by national legislation. Art. 4, sec. 3 of the GDPR expressly states that the restriction of processing means the marking of stored personal data with the aim of limiting their processing in the future. According to Recital 67 of the GDPR, methods by which to restrict the processing of personal data could be provided. Those methods should include: 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 be provided by technical means in such a way that the personal data is not subject to further processing operations and cannot be changed. The fact that the processing of personal data is restricted should be expressly indicated in the system.

The special regime of data restriction aims at achieving a reconciliation of the data subject's interest in a rectification or erasure of its personal data and, as well as to guarantee, the controller's interest in continuing to process the concerned personal data.

3.3.10 Erasure or destruction (digital or physical)[26]

The erasure consists in the deletion of data using electronic tools.

26 Eur. Court of HR, Rotaru v. Romania, judgment 4 January 2000, application no. 28341/95.

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 destruction is the activity of definitive elimination of data.

The GDPR provides specific provisions, which should ensure the right of the data subject to be forgotten.

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: Fundamental Principles relating to processing of personal data

The general principles for processing of personal data are stated in Art. 5 of the GDPR. The application of these ground rules on the activities of the judiciary cannot be usefully separated from a broader understanding of their notions in the context of their implementation in the judicial system as a whole. Therefore, a detailed explanation on the principles explicitly for the purposes of this project can be found in the Appendix of this document.[27] Furthermore, the principles are also reflected in many respects in the following more specific discussions.

[27] See Appendix: Fundamental principles relating to data 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.

Chapter 5: Lawfulness of processing

In the tradition of the former data protection directive[28] (DPD) and in accordance with the principles of data processing, the GDPR remains true to the concept that personal data may only be processed with the consent of the data subject concerned or some other explicit legitimate ground.[29] Such legal basis is exhaustively numerated either in Art. 6 or, in case of sensitive data, in Art. 9.

5.1. Legal basis pursuant to Art. 6

Since the judiciary processes data under the GDPR for the purpose of fulfilling its statutory functions as a judge or judicial officer[30], some of the allowances provided for in Art. 6 are not applicable from the outset. There is no data processing with the consent of the data subject, since public-law data controllers are bound by the principle of the reservation of the law in connection with the requirement of certainty and therefore legally exactly defined processing powers are absolutely necessary.[31] Likewise, the processing does not take place for the performance of a contract or to carry out pre-contractual measures, as Art. 6 Para. 1 lit. b provides. Also, a processing for the protection of vital interests under the legal ground of Art. 6, Para. 1 lit. d is unlikely to be the case, since this allowance is only to be intended of secondary importance if the processing cannot be based on any other legal basis, according to Recital 46. Especially in the case of public law action, Art. 6, Para. 1 lit. e takes precedence. In addition, such a constellation is usually about the processing of sensitive data, for which then Art. 9, Para. 2 lit. c must be regarded as the *lex specialis*. Furthermore, the public authorities and thus also the judiciary cannot rely on the data protection law of the balance of interests in Art. 6, Para. 1 lit. f, insofar as the data processing takes place in the course of the performance of their tasks.[32]

[28] Directive 95/46/EC.
[29] For details of the concept see already the Judgement of the CJEU, 20 May 2003, joined cases C-465/00, C-138/01 and C-139/01 (case "Österreichischer Rundfunk").
[30] See for more details the definition of the judicial capacity in section 1 of this document.
[31] See for a rare exception in German legislation: § 81 h *Strafprozessordnung*.
[32] "Given that it is for the legislator to provide by law for the legal basis for public authorities to process personal data, that legal basis should not apply to the processing by public authorities in the performance of their tasks.", Document 5419/1/16 REV 1 p. 27 of the Council of the European Union, 8 April 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.

5.1.1. Necessity of processing for compliance with a legal obligation, Art. 6, Para. 1 lit. c

Art. 6, para. 1 lit. c, which allows processing if this is necessary for compliance with a legal obligation to which the controller is subject, could be considered as the most frequent admission requirement for legitimate data processing by the judiciary. The determination is identical to the provision in the prior DPD. According to Art. 6, para. 3, the rule itself does not constitute an independent legal basis, but necessarily requires further specification by EU or national law.[33]

Typical examples[34] for data processing for compliance with a legal obligation:

- Information obligations of telecommunication providers towards security authorities.
- Record and retention obligations in commercial, tax and social law.
- Labour regulations that serve the observance of legally prescribed working conditions.[35]

On the basis of these examples, it becomes clear that the provision is closely related to the legal ground of Art. 6 Para. 1 lit. e, which inversely regulates the data processing by authorities in the aforementioned examples and thus regularly represents the more specific legal basis for official acts.[36] Even if Art. 6, Para. 1 lit c therefore primarily addresses private-law data controllers, processing by public-law data controllers is by no means completely excluded under this legal ground.[37]

5.1.2. Necessity of processing for the performance of a task carried out in the public interest or in the exercise of public authority vested in the controller, Art. 6, Para. 1 lit. e

The central provision for data processing by the judiciary is thus found in Art. 6, para. 1 lit. e. Again, it is necessary to observe Art. 6, para. 3, according to which it is necessary to specify the permit by means of EU or national law, which in turn provides the proper legal basis for lawful processing. The requirements for such a specification are given on the one hand by the GDPR itself (especially Art. 6,

[33] See also Rec. 45.
[34] The examples are taken from: *Buchner/Petri*, in: Kühling/Buchner, Datenschutz-Grundverordnung, *C.H. Beck*, Munich 2017, Art. 6, para. 96 et Seq.
[35] See Judgement of the CJEU, 30 May 2013, C-342/12 (case "Worten").
[36] See *Buchner/Petri*, in: Kühling/Buchner, Datenschutz-Grundverordnung, *C.H. Beck*, Munich 2017, Art. 6, para. 78.
[37] See *Heberlein*, in: Ehmann/Selmayr, Datenschutz-Grundverordnung, *C.H. Beck*, Munich 2017, Art. 6, para. 15; *Schulz*, in: Gola, Datenschutz-Grundverordnung, *C.H. Beck*, Munich 2017, Art. 6, para. 42.

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.

Para. 2 and 3) and on the other by the respective constitutional law of the Member State. Thus, at this point, the GDPR has the character of a directive rather than a regulation and naturally gives the Member States a certain leeway for implementation.

5.2. Legal basis pursuant to Art. 9

The processing of special categories of personal data, so-called sensitive data[38], is only exceptionally permissible under the restrictive conditions of Article 9. This provision therefore also reflects the risk-based approach of the GDPR.[39]

Of particular relevance to the judiciary is Art. 9 para. 2 lit. f, which explicitly permits the processing of sensitive data, insofar as this is necessary for the establishment, exercise or defence of legal claims or for acts of the courts in the context of their judicial capacity. With respect to the right to an effective remedy[40], the limit of necessity is reached only when an arbitrary disclosure of sensitive data takes place, which no longer has any connection with the dispute.[41]

[38] For a detailed explanation of this term see section 3.2.4 of this document.
[39] See for the risk-based approach in the GDPR explicitly Art. 24, para. 1, Art. 32, 33, 34. See also section 6.1.1 of this document.
[40] Art. 47 of the European Charta of Fundamental Rights.
[41] See *Schiff*, in: Ehmann/Selmayr, Datenschutz-Grundverordnung, *C.H. Beck*, Munich 2017, Art. 9, para. 42; *Weichert*, in: Kühling/Buchner, Datenschutz-Grundverordnung, *C.H. Beck*, Munich 2017, Art. 9, para. 86.

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 6: Obligations of the data controller

At first glance, it seems somewhat unclear to whom the position of the data controller in data processing within the judiciary should be specifically assigned to. Both the court or the authority as well as the individual judge or judicial officer personally come into consideration.

If data processing by judges takes place for the purpose of fulfilling the judicial tasks, there is, as a rule of judicial independence, a sovereign activity without instruction obligation. This includes all judicial tasks related to the decision-making, including all preparatory and implementing measures.[42] Even if this argues for a separate commitment as the data controller, judges form only one part of the court's panel and therefore act from a data protection perspective within the framework of the tasks assigned by the court. Therefore, the court as an association of all judges is the supervisory data controller.[43] The same applies to all other judicial employees, who also represent only a part of their respective governmental body. From an organizational point of view, some Member States even have a hierarchical authority regarding their judicial employees, which leads directly to a processing as persons who, under the direct authority of their government agency, are authorised to process personal data[44].

However, with respect to the perspective of the further investigation, it should be noted that the actions of the individual judge or judicial officer reflects the typical activities of the respective governmental agency, not only because of their number but most of all because of their characteristic function. Accordingly, the assessment of the lawfulness of the data processing bundled under the jurisdiction of the court or the agency as a data controller focuses on the processing of data by the said persons. As a result, the perspective of the data controller is central to the processing of data by judges and judicial staff.

---

[42] For details on the scale of "courts acting in their judicial capacity" see *Körffer*, in: Paal/Pauly, Datenschutz-Grundverordnung, *C.H. Beck*, 2. edition, Munich 2018, Art. 55, para. 5 et Seq.
[43] The wording of Art. 37, para. 1 lit. a, Art. 55, Para 3 and Recital 20 p. 2 supports this result, since it refers explicitly to courts and authorities and not to a single judge; For an overview of the different roles of judges in MS see https://e-justice.europa.eu/content_legal_professions-29-en.do (last accessed on 14 February 2018).
[44] See Art. 29.

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 comparison to the former DPD, the GDPR places numerous, more or less specific requirements on the data controller which must be observed in order to achieve lawful data processing. The overarching objective of this list of obligations is to ensure processing in accordance with the fundamental principles of Article 5 and thus to guarantee an adequate level of protection for the data subject. The obligations of the data controller can be differentiated between organisational, technical and institutional obligations as well as notification obligations in case of a breach of the protection of personal data. In addition, above all, the rights of the data subjects are to be considered, from which inversely arise obligations for the data controller.

6.1. Organisational obligations

The scope of the organisational duties of the data controller includes the basic assignment of the responsibility for data processing (Art. 24), the necessary establishment of a record of processing activities (Art. 30), the guarantee of appropriate data security (Art. 32), the necessity of a data protection impact assessment (Art. 35), the requirements for the selection of a data processor[45] (Art. 28), and cooperation with supervisory authorities (Art. 31).

6.1.1. Responsibility of the controller, risk-based approach

The starting point is the general clause of Art. 24, which sets out a basic standard for the duties of the data controller and explicitly emphasizes the risk-based approach that characterizes the GDPR in particular. What this means is that all circumstances of data processing must always be guided by the degree of objective risks for the data subject and their likelihood of occurrence.[46] According to Art. 24, Para. 1 p. 1, the nature, extent, and circumstances and purposes of the processing should be used as additional parameters for such a risk analysis.[47] In this context, Rec. 75 lists, by way of example, possible risks to the data subject that the controller should be aware of when processing. The data controller should take into account that, as a result of improper data processing, the data subject may suffer economic or social disadvantages, including discrimination, identity theft or fraud, financial loss,

[45] See for the delimitation of both categories section 3 of this document.
[46] See Rec. 76.
[47] *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.

reputational damage or a betrayal of professional secrets. In addition, an increased risk must naturally be taken into account when processing sensitive data[48], as well as in the case of processing the data of particularly vulnerable persons, such as minors.

In the event of improper data processing within the judiciary, there is a particularly significant risk of social disadvantage for the data subject in the form of future discrimination or reputational damage.

The risk analysis resulting from such a consideration process is not only conceptually but also methodologically closely related to the data protection impact assessment in Art. 35, as the similar wording of the two Articles makes clear.[49] If the risk analysis to be carried out prior to each data processing clearly identifies a high risk, then a detailed data protection impact assessment in accordance with Art. 35 is mandatory.[50]

With regard to the technical and organisational measures to be taken, Art. 25 (data protection by design and by default) and Art. 32 (data security), in particular, represent the more specific norms and thus displace the *lex generalis* in this respect. However, Art. 24, Para. 1 p. 2 also directly implies the obligation to review and, if necessary, update all measures taken. The limiting feature of the requirement is to be understood on a case-by-case basis, i. e. a review is required whenever, for example, legal regulations have changed, judicial or regulatory decisions on the legality of processing have been taken or new approved codes of conduct or certification procedures have been approved.[51] An involvement of the judicial data protection officer to observe the current factual and legal situation stands to reason.

In addition, Art. 24, Para. 1 p. 1 addresses the obligation of the data controller to provide evidence of lawful processing. In particular, Art. 5, Para. 2 (accountability) and Art. 30 (records of processing activities) are the more specific provisions for this rather general wording.

[48] For a detailed explanation of this term see section 3.2.4 of this document.
[49] See also *Hartung*, in: Kühling/Buchner, Datenschutz-Grundverordnung, *C.H. Beck*, Munich 2017, Art. 24, para. 16.
[50] See for further details section 6.1.4 of this document.
[51] See *Bertermann*, in: Ehmann/Selmayr, Datenschutz-Grundverordnung, *C.H. Beck*, Munich 2017, Art. 24, para. 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.

Art. 24, Para. 2 emphasises that the principle of proportionality[52] applies to the introduction of appropriate internal and external data protection policies (in the sense of establishing specific rules for handling personal data). Such data protection policies are recognised as a concrete organisational measure in accordance with Art. 24, para. 1. Due to the explicit emphasis in a separate paragraph, it is to be assumed that the definition of a data protection policy by the data controller must at least to be considered.

As with many other provisions of the GDPR[53], Art. 24, para. 3 provides that the application of approved codes of conduct (Art. 40) or the implementation of an approved certification procedure (Art. 42) can be regarded as an indication of lawful processing. Accordingly, such self-regulation does not guarantee data processing in accordance with the GDPR. With regard to self-regulation by the judiciary, it should be noted that there is no possibility for public authorities to introduce codes of conduct, which also results from the lack of monitoring possibilities pursuant to Art. 41, para. 6.[54] Nevertheless, approved codes of conduct from other entities can at least serve as a useful guide.

6.1.2. Record of processing activities

Pursuant to Art. 30, Para. 1 p. 1, each data controller is obliged to keep a written record of all processing activities in order to, if necessary, be able to prove compliance with the data protection regulations of the GDPR.[55] This constitutes a concretisation of the accountability already mentioned in Art. 5, Para. 2 and Art. 24, Para. 1. In contrast to the former DPD, there is therefore no longer a general obligation to report to the supervisory authority.[56] Here again, the risk-based approach of the GDPR becomes evident.

Such a record must contain, for each processing activity separately, the items listed in Art. 30 para. 1 p. 2. The term "processing activity" is not to be equated with the term "processing" as defined in Art.

[52] Art. 52, para. 1 of the European Charta of Fundamental Rights.
[53] See also Art. 25, para. 3; Art. 28, para. 5; Art. 32, para. 2.
[54] See *Schweinoch/Will*, in: Ehmann/Selmayr, Datenschutz-Grundverordnung, *C.H. Beck*, Munich 2017, Vorb. Art. 40, para. 10, Art. 41, para. 31; *Paal*, in: Paal/Pauly, Datenschutz-Grundverordnung, *C.H. Beck*, 2. edition, Munich 2018, Art. 41, para. 21.
[55] See Rec. 82.
[56] See Art. 18 and 19 of the former DPD.

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 Para. 2, but rather usually comprises a number of processing steps.[57] A summary such as this ensures a reasonable degree of clarity so that the possibility for the supervisory authorities to inspect the list provided for in Art. 30, Para. 4 does not fail from the outset due to its scope and small scale.[58]

Under Article 30, institutions—among which, conceptually, institutions of the judiciary are included[59]—with fewer than 250 employees are fundamentally exempt from maintaining a record of processing operations. However, this applies only if there is no increased risk to the rights and freedoms of the data subject and the processing is only occasional and does not involve sensitive data[60]. All judicial institutions will have to keep a compulsory record of their processing activities, not least in view of the fact that data processing is carried out on a regular, and not just occasional, basis.

6.1.3 Security of processing

The central provision in this case is Art. 32, which establishes a total of eight criteria for achieving data security that must be taken into account when determining appropriate technical and organisational measures in order to ensure a level of protection commensurate with the risk:

- Type of processing.
- Extent of processing.
- Circumstances of processing.
- Purposes of processing.
- Level of risk to the rights and freedoms of the data subject.
- Probability of risk occurrence.
- State of the art.
- Amount of implementation costs.

[57] See Art. 24, para. 2; Art. 28, para. 4; Art. 35, para. 6.
[58] See *Hartung*, in: Kühling/Buchner, Datenschutz-Grundverordnung, *C.H. Beck*, Munich 2017, Art. 30, para. 14 et Seq.
[59] See *Martini*, in: Paal/Pauly, Datenschutz-Grundverordnung, *C.H. Beck*, 2. edition, Munich 2018, Art. 30, para. 27.
[60] For a detailed explanation of this term see section 3.2.4 of this document.

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.

What is striking in this enumeration is that the first six of the above-mentioned parameters must already be taken into account in the risk prognosis specified in Art. 24 and that, in keeping with the risk-based approach, a substantive link is thus created between the risk analysis be carried out *ex ante* and data security. However, the question of suitable measures must also take into account the state of the art and the amount of implementation costs. State-of-the-art technology refers to such precautions that correspond to what is currently technically possible, are based on sound scientific knowledge, as well as being practicable and available for implementation.[61] Ensuring the up-to-datedness of technologies used naturally implies an obligation to regularly review the measures taken. The amount of implementation costs, on the other hand, serves as a limiting feature and is intended to ensure that costs and risks are in an economically reasonable relationship.

Specific examples of suitable security measures are also listed in Art. 32 Para. 1. In view of the risks to the data subject resulting from the processing of personal data by judges, pseudonymisation[62] of personal data should always be considered, unless mandatory statutory provisions exclude such pseudonymisation. A state-of-the-art level of IT security and resilience of the systems used, as required by Art. 32 Para. 1 lit. b, is also essential as a basic prerequisite for data security, and not only within the judiciary. Particularly in the context of ongoing digitisation, appropriate backup and recovery strategies must also be considered to prevent complete data loss in the event of technical or physical incidents. In addition, the introduction of an internal audit procedure that examines the effectiveness of the measures taken at regular intervals, as provided for in Art. 32 Para. 1 letter d, ensures a consistent level of data security in the long term and is therefore also useful for all legal processes.

For further suitable possibilities for the establishment of data security, including—and especially—in the judiciary, the enumeration in Art. 29 Para. 2 of Directive 2016/680 offers a number of quite helpful indications.

[61] See *Martini*, in: Paal/Pauly, Datenschutz-Grundverordnung, *C.H. Beck*, 2. edition, Munich 2018, Art. 32, para. 56; *Piltz*, in: Gola, Datenschutz-Grundverordnung, *C.H. Beck*, Munich 2017, Art. 32, para. 18.
[62] For a detailed explanation of this term see section 3.2.3 of this document.

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.

6.1.4. Data protection impact assessment

As already explained under 6.1.1, a data protection impact assessment (DPIA) according to Art. 35 is to be carried out whenever the risk prognosis within the meaning of Art. 24 is likely to entail a high risk to the rights and freedoms of the natural person. Here again, the risk-based approach of the GDPR becomes evident. In the same way as the basic risk prognosis, the much more comprehensive DPIA must be carried out prior to data processing.

Admittedly, with regard to data processing operations within the judiciary, one of the examples of the rules set out in Art. 35 Para. 3 is not necessarily fulfilled; however, according to Recital 91, in the case of client data processing by only one lawyer, it can be assumed that a DPIA needs not necessarily to be carried out. Conversely, if we now take into account the large number of data processing operations carried out under the umbrella of the respective court or judicial authority as the data controller in the judicial sector, then the requirement of a DPIA implementation is very likely.

The implementation of a DPIA therefore only seems to be avoidable if a so-called negative list in accordance with Art. 35, Para. 5 encompasses the corresponding processing operations and the procedure is thus explicitly no longer necessary.

With regard to the scope of the DPIA, at least those aspects listed under Art. 35 Para. 7 must be taken into account. It is recommended that the individual steps be performed in the order specified there.[63]

6.1.5. Responsibility of the data controller regarding the appointment of data processors

The duties of the data controller with regard to the selection and monitoring of the data processor are specified in greater detail in Art. 28 para. 1.[64] In terms of data processing within the judiciary, it is conceivable—in principle—for example, to consult specialists employed by private-sector companies

[63] For further developments regarding the detailed procedure for a data protection impact assessment see: *Estelle De Marco* in *Estelle de Marco* et. al., Deliverable D2.4a – Privacy impact assessment of the MANDOLA outcomes – MANDOLA project (Monitoring and Detecting OnLine Hate Speech), GA n° JUST/2014/RRAC/AG/HATE/6652, version 2.4a.2 of July 2017, available at http://mandola-project.eu/publications/ (last accessed on 14 February 2018).
[64] See for a definition of data controller and data processor chapter 3 of this document.

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.

for system maintenance purposes and who thus act as data processors on behalf of the respective government agency. An agreement of this kind always necessitates a contract that meets the requirements set out in Art. 28 Para. 3.

When selecting data processors, it is essential to ensure that they can guarantee a sufficient degree of data security in the form of suitable technical and organisational measures.[65] As an indication of this, data processors may benefit from the application of approved rules of conduct (Art. 40) or a recognised certification (Art. 42), as made clear in Art. 28 Para. 5. In view of the sensitive nature of the sovereign activities of the judiciary, which are subject to stricter requirements, such quality criteria should be assumed with regard to the reliability of the data processors.

Monitoring of data processors in the sense of a review of their activities is not explicitly provided for in Art. 28, para. 1. However, a requirement that the data controller be granted extensive control options results indirectly from the contractual obligations of the data processors pursuant to Art. 28, para. 3 p. 2 lit. h. In addition, the accountability of the data controller resulting from Art. 5, Para. 2 and Art. 24 already requires a regular review of the data processor.[66]

6.1.6. Cooperation with data protection authorities

Pursuant to Art. 31, the data controller (as well as the data processor) has a fundamental obligation to cooperate with the supervisory authorities when they make a corresponding request. However, a more concrete definition of this obligation only arises from the tasks (Article 57) and prerogatives (Article 58) of the supervisory authority.

When it comes to the competence of the supervisory authority, Art. 55, Para. 3 must be taken into account, which precludes the jurisdiction of the ordinary supervisory authorities in adjudication to ensure judicial independence.[67] Instead, it is intended that separate bodies be created in the judicial system of the Member States, which will be responsible for supervising the judicial activities under

[65] See also Rec. 81.
[66] See *Hartung*, in: Kühling/Buchner, Datenschutz-Grundverordnung, *C.H. Beck*, Munich 2017, Art. 28, para. 60.
[67] See Rec. 20. For more details on the meaning of Rec. 20 see section 2.4 of this document.

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 protection law.[68] As far as can be seen, no such bodies for self-regulation of the judiciary are ready for implementation in any Member State for the due date of May 25th 2018.

6.2. Technical obligations

The provisions under Art. 25 have no comparable predecessor provisions in the DPD and therefore place previously unknown, primarily technical requirements on the data controller. The standardised concepts of data protection by design (Art. 25, para. 1) and data protection by default (Art. 25, para. 2) are aimed at the conception and development of data processing products, i. e. at a stage prior to the actual data processing.[69]

With regard to the processing of judicial data in the performance of its judicial functions, the direct scope of this provision appears to be very limited, at least from a technical point of view, because in many cases these processes do not involve the use of technical products which could be appropriately configured. At best, a data protection-friendly technology design would be conceivable within the framework of the collection of evidence.

On the other hand, the provision is more relevant to the administration of justice, which in any case must align its internal data processing operations, insofar as these are IT-based, with the above-mentioned maxims.

6.3. Institutional obligations

In principle, Art. 37, Para. 1 lit. a always provides for the appointment of a data protection officer at public authorities. However, judicial activity in courts is explicitly excluded from this obligation. According to Recital 97, this also applies to independent judicial authorities, but only insofar as their judicial activity is affected.

Therefore, both courts and independent judicial authorities are in any case obliged to designate a data protection officer with regard to their other activities, such as the performance of judicial

[68] See Rec. 20.
[69] See *Baumgartner*, in: Ehmann/Selmayr, Datenschutz-Grundverordnung, *C.H. Beck*, Munich 2017, Art. 25, 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.

administration tasks.[70] Depending on the size and organisational structure of the institutions, a joint data protection officer may also be appointed.[71]

The relevant provisions on the status and equipment of the data protection officer are contained in Art. 38. Above all, it is important to ensure that the data protection officer is involved in data processing operations and all related issues at an early stage so that he or she can actually fulfil his or her obligations to advise and monitor the data controller (Art. 39, Para. 1).[72] Therefore, involvement of the data protection officer should be included as early as the planning and design stage of data processing.[73]

6.4. Reporting obligations

If a personal data breach[74] has occurred, the data controller is subject to reporting obligations to the supervisory authority (Art. 33) and notification obligations to the data subject (Art. 34).

In line with the risk-based approach of the GDPR, these notification obligations are also closely linked to the respective risk that the data subject is exposed to by disclosing personal data. Immediate notification to the supervisory authority is required in accordance with Art. 33, Para. 1 if there is a risk to the rights and freedoms of the data subject. Pursuant to Art. 34, only in the case of a high risk does the obligation to inform the data subject immediately concern the data controller itself. The latter obligation may, according to Art. 23, Para. 1 lit. f, be restricted by Member States' regulations in order to preserve the independence of the judiciary and to protect legal proceedings, provided that they comply with the principle of proportionality[75], respect the essential content of fundamental rights and freedoms and also comply with the specific provisions of Art. 23, para. 2.

[70] See *Bergt*, in: Kühling/Buchner, Datenschutz-Grundverordnung, *C.H. Beck*, Munich 2017, Art. 37, para. 17.
[71] Art. 37, para. 3.
[72] Art. 38, para. 1.
[73] See *Paal*, in: Paal/Pauly, Datenschutz-Grundverordnung, *C.H. Beck*, 2. edition, Munich 2018, Art. 38, para. 4; *Heberlein*, in: Ehmann/Selmayr, Datenschutz-Grundverordnung, *C.H. Beck*, Munich 2017, Art. 38, para. 8.
[74] See the legal definition in Art. 4 sec. 12.
[75] Art. 52, para. 1 of the European Charter of Fundamental Rights.

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 necessary risk assessment should therefore ideally be based on the most concrete set of criteria possible, which itself should be developed in line with practical experience.[76] A recourse to the results of the risk analysis to be carried out prior to the start of the data processing in the sense of Art. 24, para. 1 as well as the data protection impact assessment to be carried out, if any, according to Art. 35, appears to be advisable here.

For the judiciary, it should be noted in this context that the notification must be made to the competent supervisory authority. If there is a personal data breach in the course of judicial activities, the supervisory authority to be established separately, as described in Recital 20 above, must be informed. If the data has been disclosed as part of the judicial administration activity, the report must be sent to the "regular" supervisory authority.

6.5. Awareness and guarantee of the rights of the data subject

In addition to their general obligations in data processing, data controllers must also take into account the rights of the data subject as defined in Articles 12 to 22 in order to be able to react appropriately to them in the event of the exercise of those rights.

In principle, the Regulation grants the data subject the following rights:

- Right of information (Art. 13 and 14);
- Right of access (Art. 15);
- Right to rectification (Art. 16);
- Right to erasure ('right to be forgotten') (Art. 17);
- Right to restriction of processing (Art. 18);
- Right to data portability (Art. 20);
- Right to object (Art. 21).

From the perspective of the judiciary, with regard to the specific scope of the rights mentioned above, the opening clause of Art. 23 Para. 1 lit. f is of crucial importance. The provision determines for

[76] *Hladjk*, in: Ehmann/Selmayr, Datenschutz-Grundverordnung, *C.H. Beck*, Munich 2017, Art. 33, para. 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.

Member States the possibility of enacting restrictive legislation if it protects the independence of the judiciary and judicial proceedings, as long as it is in compliance with the principle of proportionality[77], the preservation of the essential content of the (European) fundamental rights and freedoms and the observance of the specific provisions of Art. 23, Para. 2. Accordingly, a restriction is only possible if the exercise of the rights of the party concerned threatens to impair judicial independence or the conduct of court proceedings. Especially in the latter case, it is conceivable that the rights aimed at transparency could be restricted in order to guarantee an objective investigation of the facts and to ensure equal opportunities for those involved in the proceedings.[78]

In addition, there are other opening clauses[79] which allow for certain restrictions on the rights of the persons concerned, but do not envisage specific judicial activities.

[77] Art. 52, para. 1 of the European Charter of Fundamental Rights.
[78] See *Bäcker*, in: Kühling/Buchner, Datenschutz-Grundverordnung, *C.H. Beck*, Munich 2017, Art. 23, para. 24.
[79] See Art. 14, para 4 lit. d; Art. 17, para. 3 lit. b.

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 7: Obligations of the data processor

The statements made thus far have made it clear that the position of the data controller is of central importance to the data processing activities of the judiciary. In particular, due to the independence of the judiciary, it appears highly unlikely that there is no case of action as a data controller or as a person under his or her responsibility within the meaning of Article 29. [80]

In general, data processing in the context of public law action should rarely lead to a situation in which the public-law entity is in the position of data processor[81] i. e. the processing is carried out on behalf of a separate data controller. A concrete example of this would be statutory registration activities.[82]

Nevertheless, a brief overview of its position in the regulatory structure of the GDPR should also be given in view of the more practice-relevant ordering of contract data processors by the judiciary.

Data processors also have their own obligations with regard to their processing activities, which are basically independent of those of the data controller.

The starting point is the provision of Art. 28 and not Art. 24 and Art. 25, which are addressed directly only to the data controller. However, Art. 28 Para. 1 at least implies an indirect obligation for the data processor to comply with the GDPR requirements, because only in this case is the data controller permitted to cooperate with the data processor.

On the other hand, data processors are directly obliged to maintain a register of their processing activities in accordance with Art. 30, Para. 2. The data processor is also directly responsible for ensuring adequate data security in accordance with Art. 32, Para. 1.

According to Art. 28, Para. 2, the data processor is only allowed to include further data processors in the processing of the data with the appropriate permission of the data controller. Even after approval

[80] See section 3.1.2 and section 6.1 of this document.
[81] See for a description of this term section 3.1.2 of this document
[82] See for an example in German legislation: § 2, para. 5 *Bundeskriminalamtgesetz*; See *Martini*, in: Paal/Pauly, Datenschutz-Grundverordnung, *C.H. Beck*, 2. edition, Munich 2018, Art. 28, para. 26.

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.

has been granted, the first contract data processor is still liable to the data controller for any misconduct of the second data processor pursuant to Art. 28, Para. 4 p. 2. Ordinary employees of the data processor are not to be regarded as further data processors, but only as persons acting under their supervision within the meaning of Art. 29.

This brief description makes it clear that the GDPR intends a close connection between data controller and data processor. On the one hand, this imposes certain auditing obligations on the data controller, but on the other hand it also ensures that the data processor's activities are carried out in accordance with the specifications of the regulation. Art. 28, para. 10 has a limiting effect in this context, as it automatically moves the data processor into the position of the data controller in the event of an infringement on the part of the data processor, thus assigning him or her independent responsibility.

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 8: Administrative fines

Compared to the former DPD[83], the significantly extended scope of sanctions of the GDPR are supremely evident. For example, in the case of serious violations of central provisions, up to 20 million euros may be fined pursuant to Art. 83 Para. 5. This is the case, for example, when there is a flagrant violation of the principles of data processing[84] governed by Art. 5. However, there is also the possibility of imposing a fine of up to ten million euros in the event of serious violations of the data controller's or data processor's duties[85] regulated in Art. 25 to 39.

As a matter of principle, Art. 83 does not distinguish between private law and public law action. Even if it appears very unusual from a constitutional point of view to impose a fine on another public entity, possibly even the same legal entity, this would make sense in terms of effective enforcement of data protection law, for example, to withdraw funds from a government agency operating unlawfully.[86] Against this background, the importance of the comprehensive independence of supervisory authorities once again becomes particularly apparent.

However, Art. 83, Para. 7 provides for the possibility for Member States to restrict sanctions against public authorities by their own legislation. Based on the wording of the opening clause and its reference to Art. 58, Para. 2 some experts hold the view that Member State law may only modify the fines imposed on public authorities and not waive them in full, since such restrictive legislation must not eliminate the powers of the supervisory authorities to impose sanctions.[87]

Nevertheless, most Member States will probably make use of the opening clause with reference to the principle of legality of administration and exclude fines against public authorities.[88]

[83] Directive 95/46/EC.
[84] See appendix for details on the fundamental principles.
[85] See section 6 of this document.
[86] See *Bergt*, in: Kühling/Buchner, Datenschutz-Grundverordnung, *C.H. Beck*, Munich 2017, Art. 83, para. 26.
[87] See *Nehmitz*, in: Ehmann/Selmayr, Datenschutz-Grundverordnung, *C.H. Beck*, Munich 2017, Art. 83, para. 47.
[88] See for instance the German legislation in § 43, para. 3 *Bundesdatenschutzgesetz neue Fassung.*

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 9: Conclusion

The explanations have shown that the upcoming implementation of the GDPR generally further clarifies data protection requirements, which inevitably has an impact on the data processing activities of the judiciary. However, it has also become clear that many of the new requirements are not yet sufficiently precise in themselves and that it will therefore take some time before a satisfactory level of legal certainty can be achieved. At present this means that ensuring an adequate level of data protection is highly dependent on the circumstances of the case and cannot be easily abstracted. In this respect, the further interpretation of the rules will depend largely on the opinions of the European Data Protection Board (Article 68 et seq.) and the case law of the CJEU.

With regard to the desired harmonisation of the level of data protection in the judicial sector, the numerous exceptions and opening clauses for Member State law intended to safeguard the independence of the judiciary pose a considerable challenge. The extent to which deviating special regulations can be expected from the member states will only become apparent in the course of the next few years due to the different national-state procedures regarding the implementation of the GDPR on the national level.

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.

Appendix: Fundamental principles relating to processing of personal data[89]

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"[90] 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[91]. 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.[92] 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*[93] (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 are now binding in every scenario, where processing of personal data within the territorial and material

[89] This analysis was developed for the INFORM project by Estelle De Marco (Inthemis, FR) and Matthias Eichfeld (University of Göttingen, DE).
[90] 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.
[91] EU Charter of Fundamental Rights, article 52, 3.
[92] 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).
[93] 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.

scope of the GDPR takes place.[94] In case of their violation claims for damages and sanctions may immediately follow.[95] 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[96], 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[97]. 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

[94] 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.
[95] See Art. 82, para. 1 and Art. 83, para. 5 lit. a GDPR.
[96] See Judgement of the CJEU, 1 October 2015, C-201/14 (case "Smaranda Bara"), para. 32 et seq.
[97] 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.

controller or by a third party. In order to use the latter legal basis a "test of legitimate interest" must 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[98] and processing of particularly sensitive data must be considered.[99] 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.[100]

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[101], and the meaning of the principle does not 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.[102]

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.[103] In other

[98] Art. 7 and 8 GDPR.
[99] Art. 9 and 10 GDPR.
[100] Art. 44 to Art. 50 GDPR.
[101] 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.
[102] See Recital 39 p. 2 et. seq. and Recital 60.
[103] 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.

words, it enables to ensure transparency as a proportionality safeguard where an imbalance remains between the controller and the data subject, despite the respect 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)[104]. This principle applies to all the information that must be provided in order to ensure a fair and transparent processing.[105] 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.[106]

As a result, the principles of fairness and transparency concern together both the method and the content of the information.[107]

[104] See Recital 39 to GDPR.
[105] See Recital 58 p. 1 and Recital 39 p. 2. See also Art. 12 para. 1 GDPR.
[106] 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).
[107] 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[108]

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.[109]

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[110], *"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"*.[111] This specification requires *"an internal assessment"* to identify and detail the kind of processing that *"is and is not included within the specified purpose"*.[112] 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.[113] In the same line, an overall purpose to cover a number of separate purposes is not compliant.[114]

---

[108] 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).
[109] 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.
[110] See Recital 39 p. 6.
[111] 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).
[112] *Ibid.*, III.1.1, p. 15.
[113] See for more examples *Ibid.*, III.1.1., p. 16.
[114] *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.[115] Nevertheless, a detailed description of the processing must be accessible via *"layered notice"* such as a link to a corresponding Internet page.[116]

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"*[117], *"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.[118] 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.[119]In this way it enables data subjects to make informed choices.[120] The important thing is *"the quality and consistency of the information provided"*[121], in addition to its accessibility.

[115] *Ibid.*, III.1.1, p. 16.
[116] Article 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation, op. cit., III.1.1, p. 16.
[117] *Ibid.*, II.2.1, p. 12.
[118] *Ibid.*, III.1.2, p. 17.
[119] *Ibid.*, III.1.2, p. 17.
[120] *Ibid.*, III.1.2, p. 17.
[121] *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).[122] 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.[123]

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".*[124]

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.[125]

---

[122] *Ibid*., II.3, p. 13.
[123] See *Heberlein,* in: Ehmann/Selmayr, op. cit., Art. 5 para. 14.
[124] Article 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation, op. cit., III.1.1, p. 20.
[125] 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*".

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.

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[126], two cumulative conditions must be satisfied: 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.[127]

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.[128]

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.[129] Since there is no indication in the GDPR except for the wording in recital 50 p. 2 for such a

---

[126] See for the former DPD: Judgement of the CJEU, 1 October 2015, C-201/14 (case "Smaranda Bara"), para. 30 et seq.

[127] 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.

[128] 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).

[129] 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,

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.

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 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.[130]

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[131]".

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.[132]

- *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*".[133]

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.

[130] See *Heberlein,* in: Ehmann/Selmayr, op. cit., Art. 5 para. 20; *Herbst,* in: Kühling/Buchner, op. cit., Art. 5, para. 49.

[131] 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").

[132] 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.

[133] 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.

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 of personal data.[134] Of course, this does not apply if the data controller is subject to a confidentiality obligation.[135]

- *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.[136] The more surprising and unpredictable further processing is for the data subject, the more indicates to an incompatibility with the original purpose.[137] 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.[138]

- *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.[139] As a result, a particularly careful examination is necessary.[140] As well, the general principles and the special requirements for the protection of sensitive data must be considered in such a further processing.[141]

---

[134] Recital 50 p. 9.
[135] Recital 50 p. 10.
[136] Recital 50 p. 6.
[137] Article 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation, op. cit., III.2.2, p. 24.
[138] Article 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation, op. cit., Annex 4, p. 56 et seq., 68.
[139] Article 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation, op. cit., III.2.2, p. 25, fn. 68.
[140] *Ibid.*
[141] 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.

- *The possible consequences of the intended further processing for the data subject, Art. 6 para. 1 lit. d:*
  Both positive and negative consequences must be taken into account for the assessment.[142] 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.[143] This applies especially if there is a risk of discrimination or damage to the reputation of the data subject.[144]

- *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[145] or "functional separation", which includes the consideration of, encryption and pseudonymisation[146] techniques and of aggregation techniques[147], in other words the consideration of measures ensuring that the "*data cannot be used to take decisions or other actions with respect to individuals*"[148]). 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…)[149].

[142] Article 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation, op. cit., III.2.2, p. 25.
[143] *Ibid.*,
[144] Recital 75.
[145] 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
[146] See the Definition in Art. 4 No. 5.
[147] Article 29 Data Protection Working Party, Opinion 03/2013 on purpose limitation, op. cit., III.2.2, p. 27.
[148] *Ibid.*
[149] *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.[150] Amongst those guarantees, lies the requirement to perform a compatibility test in order to identify all safeguards that are appropriate to the specific context[151]. Besides, any such processing must of course also comply with all the fundamental principles of Art. 5[152] 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[153] and the requirement to inform the data subject of the processing' purposes and of his or her rights.[154]

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.[155] This includes the implementation of anonymisation techniques if possible, which would cease the personal reference and thus the data would be no longer subject to data protection law.[156] Obviously, there is a

[150] Art. 89 para. 2 and 3.
[151] 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.
[152] Recital 50 p. 8.
[153] 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.
[154] Recital 50 p. 8.
[155] Recital 39 p. 9.
[156] See *Herbst,* in: Kühling/Buchner, op. cit., Art. 5, para. 58; See for the procedure of anonymization: Art. 29 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.

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.[157] Since the usage of personal data might produce legal consequences for the data subject, the data shall reflect reality at any given time.[158] 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.[159] For instance, if the processing purpose is preservation of evidence it can be necessary to process outdated data.[160]

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'.[161] 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.[162]

To ensure the concept of limitation the data controller should establish time limits for erasure and for a periodic review.[163] Pursuant to Art. 13 para. 2 lit. a, Art. 14 para. 2 lit. a and Art. 15 para. 1 lit. d the

Protection Working Party, Opinion 05/2014 on Anonymization Techniques, op. cit., 2.2.1, p. 7 et seq.
[157] Art. 5 para. 1 lit. d; Recital 39 p. 11.
[158] 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.
[159] Art. 5 para. 1 lit. d.
[160] See *Heberlein,* in: Ehmann/Selmayr, op. cit., Art. 5 para. 24; *Frenzel*, in: Paal/Pauly, op. cit. Art. 5 para. 40 et seq.
[161] Recital 39 p. 8.
[162] See Recital 26 p. 3 and 4 for further explanations on the criterion of identifiability.
[163] 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.[164] 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".[165]

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.[166] Moreover, personal data breaches must be reported to the supervisory authority (Art. 33) and, in certain situations, to the data subject (Art. 34).

[164] Art. 5 para. 1 lit. e.
[165] See also recital 39 p. 12.
[166] 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.

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. 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.[167] The extended obligation of accountability is an expression of the enhanced self-responsibility of the data controller under the GDPR.

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[168]

A specification of the notion of self-responsibility takes place in Art. 24 which requires 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

[167] 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).
[168] For further explanations on the concept of accountability see the sections of the specific obligations of data controller and data 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.

(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).[169] Nevertheless, the processor is also demanded to take appropriate technical and organisational measures to take care of the risk associated with data processing.[170]

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.[171] 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.[172] 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.[173]
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;

[169] Art. 28 para. 1.
[170] Art. 32 para. 1.
[171] 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).
[172] *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.
[173] 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.

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 way the advert is delivered; or
- the particular vulnerabilities of the data subject targeted.[174]

As a result, certain practices of targeted online advertising may have such an effect, especially when it comes to differential pricing strategies.[175]

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 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*"[176].

[174] *Ibid.*, II.B., p. 11.
[175] *Ibid.*
[176] 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.