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

Guidelines on GDPR and Directive 2016/680 aimed at judiciary

Contributing partners: CBKE, eLAW, INTHEMIS, ITTIG, LIF, MU, UCY, UGOE, UNIBA

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 leaflet are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission. [1]

INTRODUCTION OF THE DATA PROTECTION REFORM TO THE JUDICIAL SYSTEM

INFORM

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: University of Göttingen Contributions from: CBKE, ITTIG, eLAW, INTHEMIS, LIF, UCY, UNIBA, MU	May 9th 2018
Version 2	Originated by: University of Göttingen Contributions from: CBKE, ITTIG, eLAW, INTHEMIS, LIF, UCY, UNIBA, MU	May 14th 2018
Version 3	Originated by: University of Göttingen Contributions from: CBKE, ITTIG, eLAW, INTHEMIS, LIF, UCY, UNIBA, MU	May 22nd 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 leaflet are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission. [2]

Version 4	Elaboration of section 4 provided by INTHEMIS	June 19th 2018
Version 5	Reviewed by Law and Internet Foundation	July 20th 2018
Version 6	Updated by UGOE, eLaw, ITTIG	July 26th 2018
Version 7	Reviewed by Law and Internet Foundation	July 31st 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 leaflet are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission. [3]

INTRODUCTION OF THE DATA PROTECTION REFORM TO THE JUDICIAL SYSTEM
INFORM

Executive summary

As of 25th May 2018, the European data protection reform package with General Data Protection Regulation 2016/679 and Directive 2016/680 as its main components is applicable.

The INFORM Project is a cooperative effort of nine European partner organisations from Bulgaria, Cyprus, the Czech Republic, France, Germany, Italy, the Netherlands, Poland and Slovakia funded by the European Commission under the Justice Programme 2014-2020. Its focus is to contribute to the effective and coherent application of the General Data Protection Regulation 2016/679 and the Directive 2016/680 by the target groups, which are the judiciary, legal practitioners, and the court staff.

The following guidelines present the new regulations in a compact way regarding their practical application by the target groups, with special focus on the judiciary. The structure of the guidelines is largely based on the structure of the laws. Therefore, the scope of the GDPR and Directive 2016/680 will be discussed first, followed by an elaboration on the criterion of 'personal data'. Subsequently, the fundamental principles relating to processing of personal data and the lawfulness of processing is outlined. Afterwards, the data subject rights and the obligations of data controller and data processor are covered. Relevant aspects in connection with the transfer of personal data to third countries and the legal remedies available to the data subject are explained below. Finally, there is a reference to useful literature for practice.

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 leaflet are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission. [4]

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 leaflet are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission. [5]

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this leaflet 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 leaflet are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission. [7]

List of Abbreviations

CJEU	Court of Justice of the European Union
DPA	Data protection authority
DPIA	Data protection impact assessment
DPO	Data protection officer
ECHR	European Court of Human Rights
ENISA	European Union Agency for Network and Information Security
EU	European Union
GDPR	General Data Protection Regulation
HR	Human resources
ICT	Information and communication technology
IP	Internet protocol
IT	Information technology
MS	Member State

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 leaflet are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission. [8]

1. Introduction to the guidelines

1.1. Objective of the guidelines

The following guidelines aim to provide a condensed and practice-oriented overview of all relevant provisions of the GDPR and the Directive 2016/680 for the judicial sector and should therefore be an effective application aid. To ensure completeness, all fundamental contexts are discussed, but details for the judiciary are also highlighted. The structure of the guidelines is largely based on the structure of the laws in order to provide a good overview and understanding of the system. The content is mainly based on the review reports and other INFORM project documents which provide further details and references on specific issues.[1]

1.2. Definition of the judiciary

For a generally valid capture for all MS, which differ in legal and judicial cultures across Europe, a broad and universal scope for the concept of the judiciary as a target group of the INFORM project needs to be established. From an organisational point of view this should include the court, as the system of courts that interprets and applies the law, and the jurisdiction, as the official authority making legal decisions and judgements over an individual or materialistic item within a territory.

Against this background and with respect to EU law, all the bodies that have the following requirements[2] are part of the judiciary:

[1] See for further details to the mentioned documents the Appendix: Helpful literature.

[2] 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

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 leaflet are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission. [9]

- legal origin;
- the permanent nature, i.e. the circumstance that they do not exercise jurisdictional functions on an occasional basis;
- the mandatory nature of its jurisdiction;
- the contradictory nature of the proceeding;
- the fact that they apply juridical norms and do not pronounce according to equity;
- the 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.

From an 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. Due to the data protection perspective of the INFORM project, a distinction is made between judiciary and court staff as different target groups within the project, which requires further functional differentiation: in contrast to the court staff, the key criterion for the assignment to the judiciary under the INFORM project is that the focus of the respective activity is related with the privilege of judicial independence. However, since the project is to be based on a broad concept of judiciary, as already mentioned, the target group does also include investigators. Therefore, the target group judiciary in the INFORM project is the judicial authority as the complex of bodies fulfilling the roles of judges

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 leaflet are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

(individual judge or a panel of judges, professional judges or lay judges) and investigators (prosecutors[3], policy criminal investigation department).

2. Scope of application of GDPR and Directive 2016/680

2.1. Summary

This section deals with the scope of application of the GDPR and Directive 2016/680. Section 2.2 explains the subject matter and objectives, the material scope and the territorial scope of the GDPR. Section 2.3 explains the subject matter and objectives and the scope of the Directive, particularly by explaining the concept of competent authorities and the specific purposes of the Directive, i.e., the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties. At the end of each section, a flow chart is provided that can help to determine whether the GDPR or the Directive is applicable.

2.2. Scope of the GDPR

The **subject matter and objectives** of the GDPR are described in Article 1 of the GDPR. The GDPR regulates the protection of natural persons with regard to the processing of personal data and rules relating to the free

[3] With regard to the judicial independence, the situation of prosecutors differs among the MS. In most states, public prosecutors are not bound by instructions. For an overview about the situation see: https://www.coe.int/en/web/ccpe/-/report-on-the-independence-and-impartiality-of-the-prosecution-services-in-the-council-of-europe-member-states-in-2017.

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

movement of personal data (Art. 1, para. 1). The aim of the GDPR is thus twofold: on the one hand, it aims to protect fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data (Art. 1, para. 2) and, on the other hand, it aims to ensure free movement of personal data within the EU (Art. 1, para. 3).

The material scope of the GDPR is restricted 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 (or intend to form) part of a filing system (Art. 2, para. 1).

Material scope of the GDPR focuses on the processing of personal data. The concept of personal data (defined in Art. 4, sec. 1) is explained in more detail in the next chapter. The processing of personal data involves any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means (Art. 4, sec. 2 GDPR). This includes 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 of personal data.

Some forms of processing of personal data are excluded from the scope of the GDPR. For instance, the processing of personal data by a natural person in the course of a purely personal or household activity is beyond the scope of the GDPR (Art. 2, para. 2 lit. c). Hence, for personal notes the GDPR generally does not apply.

Furthermore, the GDPR applies to the processing of personal data in general, but is set aside for the processing of personal data in a criminal law context,

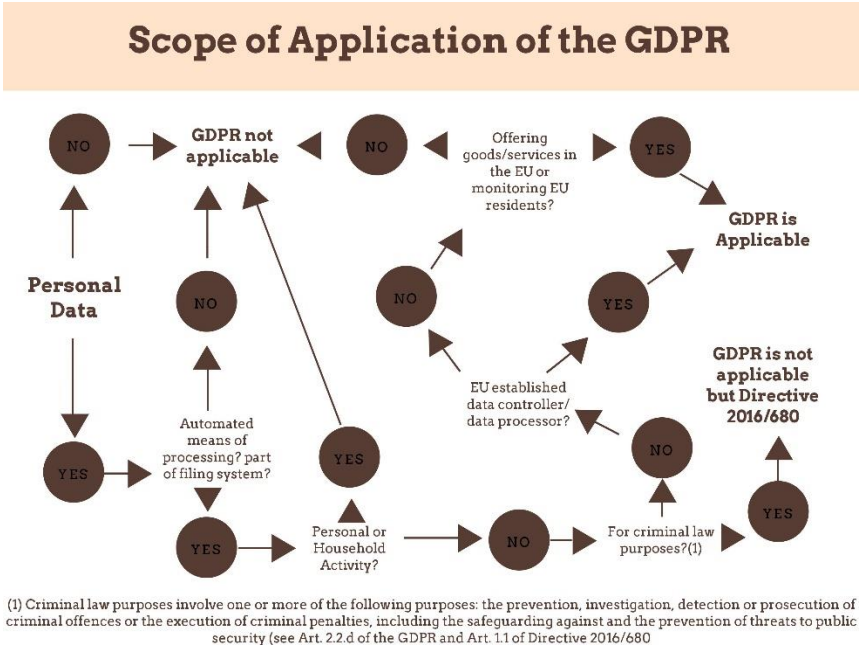
This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this leaflet are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

for the purpose 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, for which the specific rules of Directive 2016/680 apply (see Art. 2, para. 2 lit. d of the GDPR). The scope of Directive 2016/680 is explained below.

The **territorial scope** of the GPDR is restricted to the processing of personal data by data controllers and data processors established in the EU (Article 3, para. 1). This is regardless of where the data processing takes place (for instance, in the case of cloud computing). The GDPR applies to the processing of personal data of data subjects in the EU, even when processed by a controller not established in the EU, when the data processing relates to (a) the offering of goods or services to EU residents, whether for free or not, or (b) the monitoring of behavior of EU residents within the EU. It is important to note that the phrasing of the GDPR includes all EU residents, not only EU citizens.

The question whether the GDPR is applicable, can be answered using the following flow chart:

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 leaflet are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.



2.3. Scope of Directive 2016/680

Directive 2016/680 and the GDPR are related to each other as a *lex specialis* versus a *lex generalis*: As was mentioned above, the GDPR applies to the processing of personal data in general but is set aside for the processing of personal data in a criminal law context, for which the specific rules of the Directive apply (see Art. 2, para. 2 lit. d of the GDPR). The **subject matter and objectives** of the Directive are described in Article 1 of the Directive. The Directive lays down the rules relating to the protection of natural persons

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 leaflet are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

with regard to the processing of personal data by competent authorities for the following specific purposes: prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security (Art. 1). Similar to the GDPR, the aim of the Directive is twofold: on the one hand, it aims to protect fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data (Art. 1, para. 2 lit. a of the Directive) and, on the other hand, it aims to ensure the exchange of personal data by competent authorities within the EU (Art. 1, para. 2 lit. b of the Directive).

The Directive focuses on data processing by so-called competent authorities, which is defined in Art. 3, para. 7. **Competent authorities** include (a) any public authority competent for 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 and (b) any other body or entity entrusted by Member State law to exercise public authority and public powers 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.

The scope of the Directive is limited to the processing of personal data by the competent authorities for the **specific purposes** of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties (Art. 1 and 2). This includes the safeguarding against and the prevention of threats to public security (see also Recital 11). As such, it should be noted that not all personal data processed by law enforcement

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 leaflet are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

agencies and the judiciary (when processing criminal law cases) is within the scope of the Directive, as this may depend on the purposes of the data processing.

For instance, when law enforcement agencies or the judiciary are processing personnel data regarding their staff, for instance, for paying wages or assessing employee performance, the GDPR applies rather than the Directive. The GDPR is also applicable for personal data processing regarding borders, migration and asylum. Only when data are being processed in criminal procedures by these organisations, they are within the scope of the Directive.

Also, when others than the competent authorities collect and process personal data on criminal cases, these data are within the scope of the GDPR rather than the Directive. For instance, when a professor in criminal law or criminology wants to study organized crime and receives a copy of some criminal files from the judiciary, the personal data in these files kept by the professor are in the scope of the GDPR rather than the Directive. Similarly, when a private investigator ('private detective') or a journalist starts digging into a crime, he may collect personal data on suspects, criminals, witnesses, etc. These personal data kept by private investigators or journalists are within the scope of the GDPR rather than the Directive.

When a body or entity collects and processes personal data in order to comply with a legal obligation to which it is subject, the GDPR applies. For example, for the purposes of investigation, detection or prosecution of criminal offences, financial institutions retain certain personal data which are processed by them and provide those personal data only to the competent

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 leaflet are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

national authorities in specific cases and in accordance with national law (see Recital 11). These financial institutions are not considered to be competent authorities in the meaning of the directive and, therefore, are within the scope of the GDPR rather than the Directive. A body or entity which processes personal data on behalf of such authorities within the scope of the Directive should be bound by a contract or other legal act and by the provisions applicable to processors pursuant to the Directive, while the application of the GDPR remains unaffected for the processing of personal data by the processor outside the scope of the Directive. Typical examples may be tax and customs authorities, financial investigation units, independent administrative authorities, or financial market authorities responsible for the regulation and supervision of securities markets (see Recital 22).

Both data used on crimes that have already taken place (for instance, data regarding crime reconstructions and evidence for in courts) and data used on crimes that still might take place (for instance, crime prediction models that police agencies use to prevent crime)[4] are within the scope of the Directive. The data may relate to crimes, but also to suspects, criminals, victims, witnesses, testifying law enforcement officers, and police informants. In case of crime prevention, there may be suspects involved (i.e., those preparing a crime), without a completed criminal act (as it was still in preparation).[5] The crimes may be directed against specific victims, but in some cases there may

[4] See also Recital 26.

[5] Note that preparing serious crimes is a punishable offence (and hence a crime in itself) in most jurisdictions.

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 leaflet are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

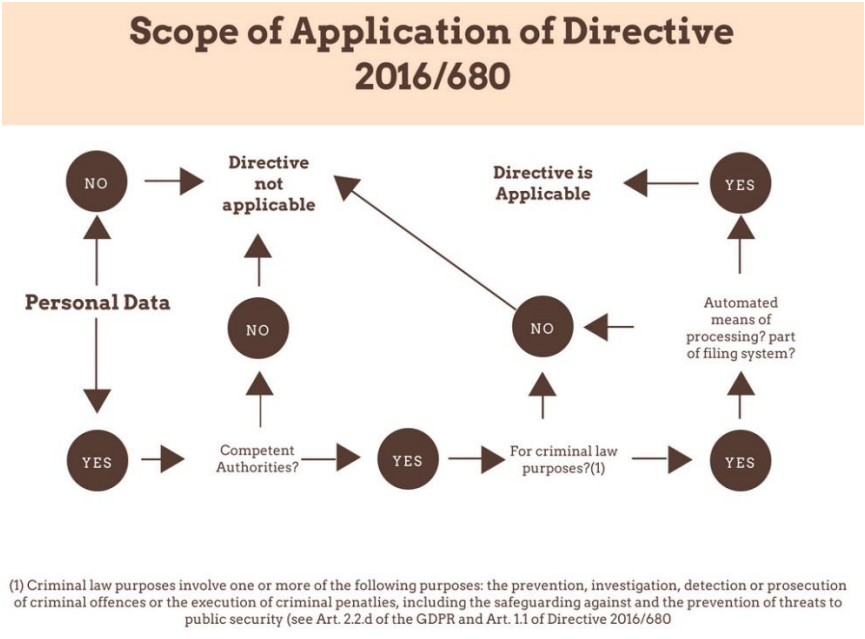
not be a specific victim. Typical examples include the possession of illegal contraband or recreational drug use.

The scope of the Directive is on the processing of personal data wholly or partially by automated means (such as personal data in databases) and non-digitalized data that is or will be part of a filing system (such as personal data in hardcopy case files).

All natural persons of whom personal data are processed within criminal law are within the scope of the Directive, regardless of nationality or residence. The Directive does not apply to the processing of personal data by EU institutions, bodies, offices and agencies (Art. 2, para. 3 lit. a of the Directive).

The question whether the Directive is applicable, can be answered using the following flow chart:

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 leaflet are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.



3. What is personal data?

3.1. Summary

Nowadays large amount of personal data is collected, processed and stored due to the high use of ICT technologies. In particular, in the world of justice the use of ICT appears as the key element to crucially improve the administration of justice and, in the meanwhile, it opens up to relevant problems related to the personal data protection field. In such context, knowing "what personal data is" represents a fundamental information which

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 leaflet are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

judiciary have to deal with when processing data in the daily activities and practices. Therefore, the correct understanding of the definition of "personal data" is of a paramount importance when it comes to the proper application of the Regulation (EU) 2016/679 (hereafter GDPR) and Directive 2016/680/EU (hereafter Directive), in order to be compliant with them. The aim of these Guidelines section is to contribute to an in-depth and accurate knowledge of the meaning of the issues (pseudonimysation, types of data, data processing) surrounding the concept of "personal data" under the GDPR and the Directive to deepen the expertise of the professionals, especially when it comes to judges, lawyers and courts staff.

3.2. Personal data

The GDPR and the Directive use a broad definition of personal data. However, the provisions go on to clearly state examples of this personal data, and specifically add new identifying types of data to its definition. Both the European measures update definitions of personal data to reflect contemporary style of living, changes in technology and the way in which organisations and companies collect and store information. The aim of this Guidelines sub-section is to contribute to an accurate knowledge of the concept of personal data under the GDPR and the Directive to deepen the expertise of the judiciary.

In particular, the relevance of concept of personal data protection within the data protection reform package is increasingly recognized. The use of ICT technologies, in the judiciary context, 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 processing of personal data: A large

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 leaflet are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

amount of personal data is collected, processed and stored by the judiciary and many implications related to data protection issues rise with respect to judiciary when processing data in their daily practices.

Legal background

The homogeneity of the definitions of "personal data" provided by the Directive (Article 3, sec. 1) and by the GDPR (Article 4, para. 1) contribute to harmonize the level of data protection between Member States. Judiciary would benefit of this consistency when processing personal data in their daily activities.

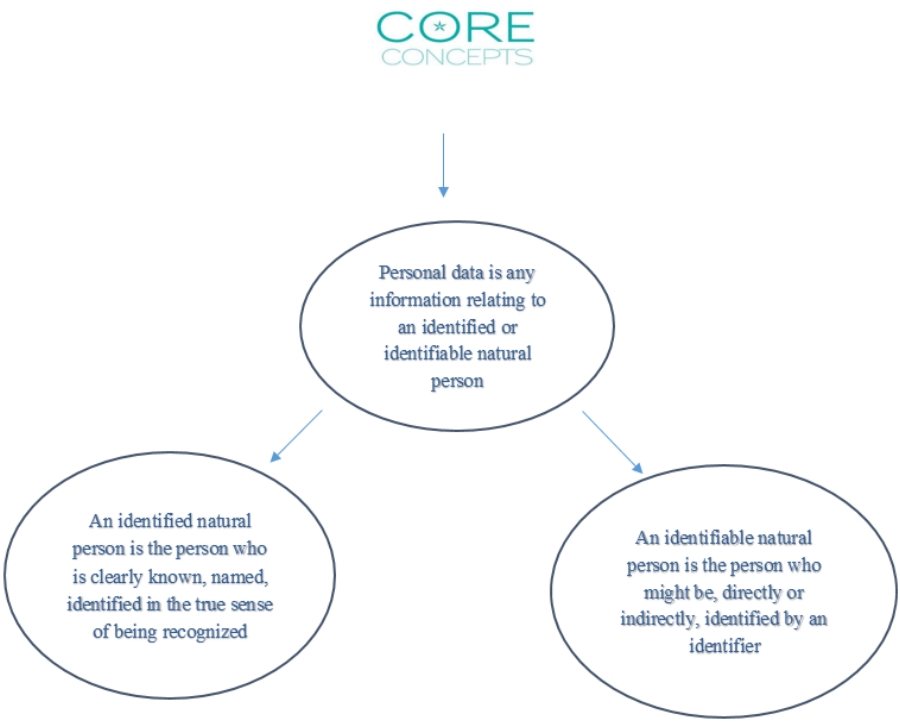
This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this leaflet are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

Directive (EU) 2016/680	*Regulation (EU) 2016/679*
Art. 3 sec. 1	Art. 4 sec. 1
Personal data means **any information relating to an identified or identifiable natural person** ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.	Personal data means **any information relating to an identified or identifiable natural person** ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

The notions of the Directive and of the GDPR reflects the intention of the European legislator for adopting a broad concept of "personal data". Data has to be "personal" in order to fall under the scope of application of the data protection rules. Therefore, the examined concept covers any sort of statements about a "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 leaflet are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission. [22]

Core concepts



In particular

Data that falls outside the application of GDPR is:

- data of deceased persons

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 leaflet are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission. [23]

- data of legal entities, including the name and the form of the legal person and the contact details of the legal person [*for further clarification see examples below*]
- anonymous data

Data that falls outside the application of Directive is:

- data of legal entities, including the name and the form of the legal person and the contact details of the legal person [*for further clarification see examples below*]
- anonymous data

Identification and identifiability occur when personal data belongs to:

- an already identified individual
- an individual who is not identified yet, therefore his or her identification is merely possible by reference to an identifier

An identifier is:

- a person's name (the most common element to directly identifies an individual)
- an identification number (the most common element to indirectly identifies individual), such as: ID number, telephone number, a social security number, a passport number, a car registration number, which might be indirectly identify a person
- a location or address

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 leaflet are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission. [24]

- an online identifier, which may involve IP addresses or cookies. This kind of identifier is provided by individual devices, internet protocol addresses, and radio frequency identification tags, just to give some practical examples

In cases where the extent of the available identifiers does not allow anyone to select specifically and univocally an individual, identification might still be possible by combining different information that by themselves would not have traced back to that individual. This is where the GDPR and the Directive comes with "one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person".

Examples

Fragmentary information in the press

"Information is published about a former criminal case which won much public attention in the past. In the present publication, there is none of the traditional identifiers given, especially no name or date of birth of any person involved. It does not seem unreasonably difficult to gain additional information allowing one to find out who are the persons mainly involved, e.g. by looking up newspapers from the relevant time period. Indeed, it can be assumed that it is not completely unlikely that somebody would take such measures (as looking up old newspapers) which would most likely provide names and other identifiers for the persons referred to in the example. It seems therefore justified to consider the information in the given example as being 'information about identifiable persons' and as such personal data." (*Source: Opinion 4/2007 Article 29 WP)*

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 leaflet are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

Legal person

The name of a legal person will be a personal data as long as this name refers or enables to refer to one single person (it will be the case for example if the company has the name of its founder, or a name that is known to be used by a single natural person who created it).

The contact details of the legal company might be personal data in case the founder established the legal entity at his/her home (the contact details also refer to a single house or phone contract owner).

When the contact details are the one of an employee, these details are professional and not private (unless they are the one of the private home), but in any case these remain personal data (since the employee is a natural person).

Relevant cases

- Judgment of the European Court of Justice, C-101/2001, of 6 November 2003 (Lindqvist case): list of various persons identified on an internet page by name or by giving their telephone number or information related to their social or working conditions[6]
- Judgment of the European Court of Justice, C-582/14 of 19 October 2016 (case Breyer): dynamic IP address[7]

Recommendation

[6] https://e-justice.europa.eu/ecli/ECLI:EU:C:2003:596?&lang=en&init=true
[7] https://e-justice.europa.eu/ecli/ECLI:EU:C:2016:779?&lang=en&init=true

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 leaflet are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission. [26]

Judiciary should have an in-depth and accurate knowledge of the meaning of the concept of personal data. Only the information which belongs to an individual is deemed personal and falls under the data protection rules.

Judiciary has to take into consideration in their daily work activity that, not only data coming from the identification through the name is personal data, but also that coming from other identifiers or the combination of them. Moreover, singling out a particular person is possible by combining such identifiers with specific characteristics (details specific to physical, mental, economic, cultural or social identity) which might be pretty conclusive in some circumstances. The information related to such identifiable person is personal data and falls under the data protection rules.

3.3. Pseudonimysation

Pseudonymisation represents a key concept that has been the topic of much discussion since the introduction of the GDPR and the Directive. In general, pseudonymisation means a safeguard for storage and processing of personal data in a modified form that requires for identification of natural person additional information, which is kept separately.

Legal Background

Pseudonymisation is 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. The homogeneity of the definitions of pseudonymisation provided by

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 leaflet are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

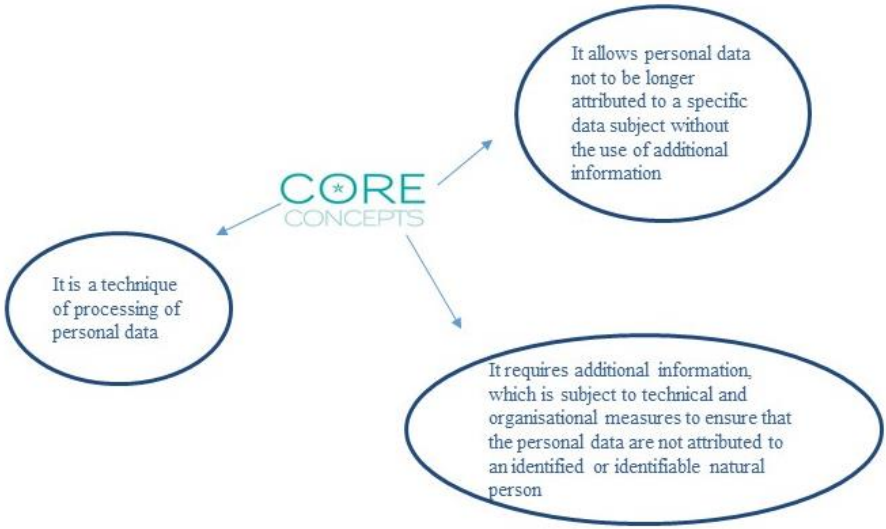
the Directive and by the GDPR contribute to harmonise the level of data protection between Member States. Judiciary would benefit of this consistency when processing sensitive personal data in daily activities.

Directive (EU) 2016/680	***Regulation (EU) 2016/679***
Art. 3, sec. 5 Pseudonymisation means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.	Art. 4, sec. 5 Pseudonymisation means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

The notions of the Directive and of the GDPR recognizes the data protection-enhancing effect of this technique when the processing activities are taken on de-identify personal data.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this leaflet are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission. [28]

Core concepts



In particular

- The data protection rules encourage to implement appropriate safeguards "both at the time of the determination of the means for processing and at the time of the processing itself." The way to do this is by pseudonymizing personal data
- Pseudonymisation is a "processing activity" that makes data no longer attributable to a specific natural person
- If pseudonymisation process is applied by judiciary, it does not have to provide data subjects with rights to access, rectification, erasure or data portability

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 leaflet are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission. [29]

- The "key" that enables re-identification of individuals is kept separate and secure, therefore the risks associated with pseudonymised data are likely to be lower
- Technical and organisational measures are provided in order to secure non attribution to a single identified or identifiable natural person

Examples

Non-aggregated data for statistics

"It has to be taken into consideration the case of personal information processed by the national institute for statistics, where, at a certain stage, the information is kept in non-aggregated form and do not relate to specific individuals. This information is designated with a code instead of a name (e.g. the individual coded X1234). The institute for statistics keeps separately the key to these codes (the list associating the codes with the names of the persons). That key can be considered to be likely reasonably to be used by the institute for statistics, and therefore the set of individual-related information can be considered as personal data and should be subject to the data protection rules by the institute. Now, we can imagine that a list with data about wine drinking habits of consumers is transferred to the national wine-producer organization in order to enable them to back up their public stance by statistical figures. To determine whether that list of information is still personal data, it should be assessed whether the individual wine consumers can be identified "taking into account all the means likely reasonably to be used by the controller or any other person". If the codes used are unique for each specific person, the risk of identification occurs whenever it is possible to get access to the key used for the encryption. Therefore, the risks of an

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 leaflet are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

external hack, the likelihood that someone within the sender's organisation - despite his professional secrecy - would provide the key and the feasibility of indirect identification are factors to be taken into account to determine whether the persons can be identified taking into account all the means likely reasonably to be used by the controller or any other person, and therefore whether information should be considered as "personal data". If they are, the data protection rules will apply. A different question is that those data protection rules could take into account whether risks for the individuals are reduced, and make processing subject to more or less strict conditions, based on the flexibility allowed by the rules of the Directive. If, on the contrary, the codes are not unique, but the same code number (e.g. "123") is used to designate individuals in different towns, and for data from different years (only distinguishing a particular individual within a year and within the sample in the same city), the controller or a third party could only identify a specific individual if they knew to what year and to what town the data refer. If this additional information has disappeared, and it is not likely reasonably to be retrieved, it could be considered that the information does not refer to identifiable individuals and would not be subject to the data protection rules." *(Source: Opinion 4/2007 Article 29 WP).*

Relevant cases

There are no relevant cases on this topic, which is a new concept in the European data protection legislation.

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 leaflet are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

Recommendation

Judiciary has to pay special attention on pseudonymisation techniques implementation. Even if no guidance on pseudonymization has been released by the European Legislator yet, judiciary, has to reach deep awareness of the existence of pseudonymisation techniques that might help them to fulfil their data security obligations. The GDPR and the Directive render more flexible several requirements on data controllers that use such technique. Judiciary has to follow the willingness of the European legislator on data protection who encourages the use of pseudonymisation as an appropriate measure for achieving data protection through the use of technology, and, in the meanwhile also maintaining the personal data's utility.

3.4. Special type of data

The GDPR and the Directive provide elevated protection for sensitive personal data, by expressly prohibiting its processing unless specific conditions apply.

Legal Background

The homogeneity of the definitions of "sensitive personal data" provided by the Directive and by the GDPR contribute to harmonise the level of data protection between Member States.

Directive (EU) 2016/680	***Regulation (EU) 2016/679***

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

Art. 10	Art. 9, para. 1
Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be allowed only where strictly necessary, subject to appropriate safeguards for the rights and freedoms of the data subject.	Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited. *(Paragraph 1 shall not apply if one of certain conditions applies)*

Both the Directive and the GDPR set out high level of protection for special categories of personal data. It has to be noticed that while GDPR provides for general rules on data protection, the Directive specifically applies to the processing of personal data only by those public authorities who are "competent" for the purposes of the prevention, investigation, detection or prosecution of criminal offences, and the execution of criminal penalties.

Nevertheless, the basis of the “sensitive personal data” concept is absolutely the same.

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 leaflet are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

The Directive and the GDPR include other provisions related to sensitive personal data, which are considered in different sections of these Guidelines (section 4, 5…).

In particular, if judiciary is processing sensitive personal data, one or more of the exemptions provided in Art. 9, Para. 2 of the GDPR and in Art. 10 lett. a, b, c of the Directive has to be satisfied, as well as one of the general conditions which apply in every case (see Art.6 of the GDPR or Art. 8 of the Directive "Lawfulness of processing").

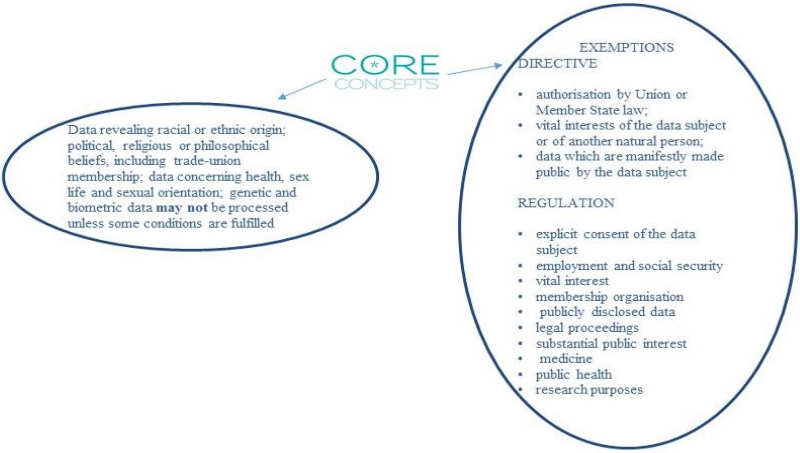
In other words, when processing sensitive personal data, judiciary needs to identify different conditions

• A lawful basis for processing under Art. 6, of the GDPR and Art. 8 of the Directive in the same way as for any other processing of personal data.

• A specific condition under Art. 9, Para. 2 of the GDPR or Art. 10 lit. a,b, c of the 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 leaflet are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission. [34]

Core concepts



In particular

Sensitive personal data, which may **not be processed** under the GDPR and Directive unless some conditions are fulfilled, is the following:

- *data revealing racial or ethnic origin* should include for example data concerning a natural person's country of origin, place of birth of parents and the native language
- *data revealing political opinions* should include information on natural person's membership in a political party, on a participation in a political reunion or similar event
- *data revealing religious or philosophical beliefs* relates to information allowing conclusions as to an individual's religious affiliation or lack thereof

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 leaflet are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

- *data revealing trade-union membership* relates to information on individuals trade union activities and should be used in a discriminatory way in the employment market
- *data concerning health* relates to the physical or mental health of a natural person, including the provisions of health care services, which should reveal information about the natural person's health status. From a judicial perspective, health data should be relevant when dealing with insurance litigation, personal injury litigation (claims for medical expense reimbursement, claims damages for lost wages or diminished employment opportunities), as well as in case of criminal investigation (expert reports on health conditions of an individual to be used in trial for evidence)
- *data concerning an individual's sex life or sexual orientation* is deemed particularly sensitive as it should include information on gender identity and for example sex characteristics disclosing that the citizen has changed the name and the sex ascribed at birth
- *genetic data*, 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
- *biometric data*, personal data resulting from specific technical processing relating to the physical, physiological or behavioral characteristics of a natural person, which allows or confirms the unique identification of that natural person, such as facial images or dactyloscopic 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 leaflet are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

Exemption from the prohibition of processing sensitive personal data under the GDPR

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 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 EU 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 leaflet are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission. [37]

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.

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 leaflet are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

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 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 of the GDPR 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:

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 leaflet are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

- 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 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

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 leaflet are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

should provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

Exemption from the prohibition of processing sensitive personal data under the Directive

- authorization by Union or Member State law. This is certainly the case of processing carried out by the judicial authority
- vital interests of the data subject or of another natural person
- data manifestly made public by the data subject

Data revealing criminal convictions

Sensitive personal data relating to criminal offences and convictions is addressed separately due to the high level of sensitivity (Art. 10 of the GDPR). Processing of personal data relating to criminal convictions and offences or related security measures, based on a legal permission under Art. 6, para. 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 leaflet are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

Examples

"The former patient A of a hospital sues the latter. The hospital uses A's medical record in order to defend itself against lawsuit. In this example, the medical record reveals data on A's health and thus, merits protection under Art. 9, para. 1 GDPR. However, the hospital uses the data to defend itself against a lawsuit of A. In this case, the processing of personal data is necessary for purposes of proof in the course of the legal proceedings. In this regard, A's right to privacy is outweighed by the necessity of processing A's data in order to submit evidence in the course of the lawsuit".[8]

Relevant cases

Source: European Court of Human Rights, Press Unit, *Factsheet- Personal data protection*. April 2018[9]:

- Collection of fingerprints records:
  Eur. Court of HR, M.K. v. France, judgment of 18 April 2013, application no. 19522/09[10]
- Collection of health data:

Eur. Court of HR, L.H. v Latvia, judgment of 29 April 2014, application no. 52019/07[11];

[8] See Voigt/von dem Bussche, *The Eu General Data Protection Regulation (GDPR). A practical Guide*, Springer International Publishing AG 2017.
[9] https://www.echr.coe.int/Documents/FS_Data_ENG.pdf
[10] http://hudoc.echr.coe.int/eng#{%22ecli%22:[%22ECLI:CE:ECHR:2013:0418JUD001952209%22]}
[11] http://hudoc.echr.coe.int/eng#{%22ecli%22:[%22ECLI:CE:ECHR:2014:0429JUD00107%22]}

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

Recommendation

Judiciary in the daily work activities must be aware that the misuse of sensitive personal data might be irreversible and have long-term consequences as well as strong impact for the natural person. For this reason judiciary, when processing sensitive personal data ought to adopt certain safeguards and to pay specific attention.

3.5. The processing of personal data

Processing include a range of operations on personal data, performed by manual or automated means. This includes the **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** of personal data. The GDPR applies to the processing of personal data wholly or partly by automated means as well as to non-automated processing, if it is part of a structured filing system.

The Directive applies to the processing of personal data by competent authorities for the purposes set out by the said Directive.

Therefore, the Directive is not limited to cross border processing but to all forms of processing falling within the objective of the said Directive. It 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.

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 leaflet are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

Legal background

The term "processing" is very broad both in the GDPR and in the Directive. It essentially means anything that is done to, or with, personal data (including simply collecting, storing or deleting those data). This definition is significant because it clarifies the fact that EU data protection law is likely to apply wherever an organization does anything that involves or affects personal data.

The homogeneity of the definitions of "processing" provided by the Directive and by the GDPR contribute to harmonize the level of data protection between Member States

Directive (EU) 2016/680	***Regulation (EU) 2016/679***
Art. 3, sec. 2 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 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.	Art. 4, sec. 2 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 as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

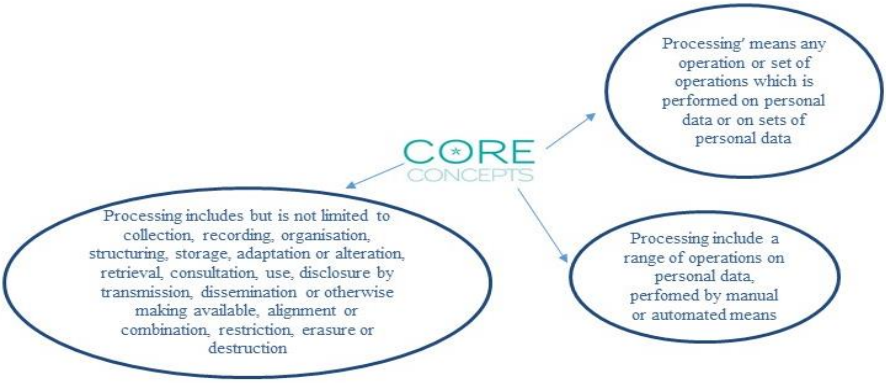
This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this leaflet are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission. [44]

Art. 3, sec. 3	Art. 4, sec. 3
'Restriction of processing' means the marking of stored personal data with the aim of limiting their processing in the future.	'Restriction of processing' means the marking of stored personal data with the aim of limiting their processing in the future.

The Directive and the GDPR include other provisions related to personal data processing, which are considered in different sections of these Guidelines (chapter 2, 4, 5...). Specifically, the general principles for processing of personal data are stated in Art. 5 of the GDPR (see chapter 4 of these Guidelines). 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.

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 leaflet are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

Core concepts



In particular

There are different types of processing:

Collection

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 authorizes 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

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 leaflet are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

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.).

Recording and storage

Recording consists in the transposition of data on electronic files. It can be preceded by the data collection which does not necessarily take place on electronic files.

Collection and recording can coincide when the recording activity is performed at the same time as the collection activity.

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. In particular, 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 organized 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 of the GDPR. It is to be noted that Art. 17 of the GDPR on the right to be forgotten, provides that this right does not apply when processing is necessary "for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller". (Article 17 para 3 let. b). This is the case of judicial authority.

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 leaflet are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

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 organized and structured data is the better is its management in terms of data protection.

Adaptation or alteration

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

Retrieval or consultation

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

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.

Use, alignment or combination

The use is a generic activity that covers any type of data use – for example, in the judiciary context the use of personal data has very broad application - when drafting judgments and other operational acts, which contain personal data, when analysing and assessing evidences, etc.

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

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 leaflet are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission. [48]

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

Disclosure by transmission

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

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 publishing personal data in a daily newspaper 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.

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 leaflet are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission. [49]

The dissemination process mainly concerns the online publication of judgments by judges, as well as the public hearings.

Restriction

Art. 4, para. 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.

Erasure or destruction (digital or physical)

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

The destruction is the activity of definitive elimination of data.

Examples

The definition of processing is very wide and it is difficult to think of anything an organisation might do with data that will not be 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 leaflet are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

Examples of processing include:

- Transfer of a case file from police to public prosecutor
- staff management and payroll administration;
- access to/consultation of a contacts database containing personal data;
- shredding documents containing personal data;
- posting/putting a photo of a person on a website;
- storing IP addresses or MAC addresses;
- video recording (CCTV) e.g., having cameras in courtrooms.

Relevant cases

Source: European Court of Human Rights, Press Unit, *Factsheet- Personal data protection*. April 2018[12]:

Collection

- Collection of fingerprints records:

Eur. Court of HR, M.K. v. France, judgment of 18 April 2013, application no. 19522/09[13].

- Collection of health data:

Eur. Court of HR, L.H. v Latvia, judgment of 29 April 2014, application no. 52019/07[14];

[12] https://www.echr.coe.int/Documents/FS_Data_ENG.pdf
[13] http://hudoc.echr.coe.int/eng#{%22ecli%22:[%22ECLI:CE:ECHR:2013:0418JUD001952209%22]}
[14] http://hudoc.echr.coe.int/eng#{%22ecli%22:[%22ECLI:CE:ECHR:2014:0429JUD005201907%22]}

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

Recording and storage

- Storage of certain information in Security Police files:

Eur. Court of HR, Segerstedt-Wiberg and Others v. Sweden, judgment of 6 June 2006, application no 62332/00[15].

- Storage in the context of criminal justice:

Eur. Court of HR, Perry v. United Kingdom, judgment of 17 July 2003, application no. 63737/00[16].

Eur. Court of HR, Peruzzo and Martens v. Germany, judgment of 4 June 2013, Applications nos. 7841/08 and 57900/12[17].

Eur. Court of HR, Da Gregorio and Mosconi v. France, judgment of 8 November 2016, application no. 65714/11[18].

Eur. Court of HR, Figueiredo Teixeira v. Andorra, judgment 8 November 2016, application no. 72384/14[19]

- Storage in the context of health:

Eur. Court of HR, L.L. v. France, judgment 10 October 2006, application no. 7508/02[20].

- Storage in secret registers:

[15] http://hudoc.echr.coe.int/eng#{%22ecli%22:[%22ECLI:CE:ECHR:2006:0606JUD006233200%22]}
[16] http://hudoc.echr.coe.int/eng#{%22ecli%22:[%22ECLI:CE:ECHR:2003:0717JUD006373700%22]}

[17] https://hudoc.echr.coe.int/eng#{%22ecli%22:[%22ECLI:CE:ECHR:2013:0604DEC000784108%22]}
[18] https://hudoc.echr.coe.int/eng#{%22ecli%22:[%22ECLI:CE:ECHR:2017:0530DEC006571411%22]}
[19] https://hudoc.echr.coe.int/eng#{%22ecli%22:[%22ECLI:CE:ECHR:2016:1108JUD007238414%22]}
[20] https://hudoc.echr.coe.int/eng#{%22ecli%22:[%22ECLI:CE:ECHR:2006:1010JUD000750802%22]}

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

Eur. Court of HR, Leander v. Sweden, judgment 26 March 1987, application no. 9248/81[21].

Disclosure by transmission

- Disclosure of personal data:

  Eur. Court of HR, Z. v. Finland, judgment of 25 February 1997, application no. 22009/93[22];

  Eur. Court of HR, Panteleyenko v. Ukraine, judgment of 29 June 2006, application no. 11901/02[23];

  Eur. Court of HR, Avilkina and Others v. Russia, judgment of 6 June 2013, application no.1585/09

Erasure or destruction (digital or physical)

- Eur. Court of HR, Rotaru v. Romania, judgment 4 May 2000, application no. 28341/95[24].

[21] https://hudoc.echr.coe.int/eng#{%22ecli%22:[%22ECLI:CE:ECHR:1987:0326JUD000924881%22]}
[22] https://hudoc.echr.coe.int/eng#{%22ecli%22:[%22ECLI:CE:ECHR:1997:0225JUD002200993%22]}

[23] https://hudoc.echr.coe.int/eng#{%22ecli%22:[%22ECLI:CE:ECHR:2006:0629JUD001190102%22]}

[24] https://hudoc.echr.coe.int/eng#{%22ecli%22:[%22ECLI:CE:ECHR:2000:0504JUD002834195%22]}

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

Recommendation

The judiciary can be involved in a wide range of data processing activities. It is important to note that data processing also includes activities that in plain language are not considered as such. For instance, data storage, data collection, consultation and dissemination are also types of data processing.

4. Lawfulness of processing – data processing principles

The principle of lawfulness[25] implies in the first instance that processing operations comply with law "*in the broadest sense*"[26], to parallel the requirements of purpose legitimacy that will also be analysed below[27].

The first laws that govern personal data processing - which constitute an interference with the right to private life and the right to personal data

[25] This Section 4 has been authored by Estelle De Marco. Some elements of the discussion are based on previous works performed by the same author in Estelle De Marco *et al.*, *MANDOLA Deliverable D2.2 - Identification and analysis of the legal and ethical framework*, version 2.2.4 of 12 July 2017, MANDOLA project (Monitoring ANd Detecting OnLine hAte speech) - GA n° JUST/2014/RRAC/AG/HATE/6652, http://mandola-project.eu/publications; Estelle De Marco *et al.*, *Deliverable D3.3 - Legal recommendations - ePOOLICE project (early Pursuit against Organized crime using envirOnmental Scanning, the Law and IntelligenCE systems)*, project n° FP7-SEC-2012-312651, version 1.3 of 10 December 2014, Section 3.1.2.3, available at https://www.epoolice.eu/.

[26] Article 29 Data Protection Working Party, *Opinion 03/2013 on purpose limitation*, 2 April 2013 (WP203), p. 20.

[27] See below, the Section 4.2.4 of the current guidelines.

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 leaflet are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

protection[28] - are the European Convention on Human rights (ECHR) and the European Union Charter of fundamental rights (EUCFR)[29].

Both these texts require that any limitation brought to the right to personal data protection respects a series of four principles: the limitation must have a specific, clear, accessible and foreseeable legal basis[30]; the limitation must pursue a legitimate aim; and the limitation must be necessary and proportionate to reach the aforesaid aim[31].

As a result, the first step is to identify the legal basis that authorises personal data processing operations. Once this legal basis is identified, the other steps will be to make sure that appropriate safeguards are taken in order to ensure that processing operations pursue a legitimate aim, and are necessary and proportionate to this aim. Legal bases that comply with the rule of law provide

---

[28] An "interference" or "limitation" is constituted as soon as a personal data is accessed or used (or a freedom protected by the wall of private life prevented to be exercised), "*no matter whether the information on the private lives concerned is sensitive or whether the persons concerned have been inconvenienced in any way*" (CJEU, *Digital Rights Ireland and Seitlinger e.a.*, joint cases C-293/12 and C-594/12, *op. cit.*, para. 33), and no matter whether this data is publicly available or not (see for instance Article 29 Data Protection Working Party, *Opinion 03/2013 on purpose limitation*, 2 April 2013, WP203, III.2.5, p.35). See Estelle De Marco, D2.10 - *Comparative study between the GDPR and Directive 95/46/EC including their relations to fundamental rights*, March 2018, INFORM project (INtroduction of the data protection reFORM to the judicial system), JUST-JTRA-EJTR-AG-2016, GA n° 763866, http://informproject.eu/fr/resultats/, Section 2.3.2, para.2.

[29] See Estelle De Marco, D2.10 - *Comparative study between the GDPR and Directive 95/46/EC including their relations to fundamental rights*, op. cit., Section 2.3.1, para. 2.

[30] See Recital n° 41 of the GDPR. See also Estelle De Marco, D2.10 - *Comparative study between the GDPR and Directive 95/46/EC including their relations to fundamental rights*, *op. cit.*, Section 2.3.2.1 and Annex, Section 1.1.

[31] See Estelle De Marco, D2.10 - *Comparative study between the GDPR and Directive 95/46/EC including their relations to fundamental rights*, *op. cit.*, Section 2.3.2.; See also for ex. Article 29 Data protection working party, *Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector* (WP 211), 27 February 2014, n° 3.3.

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

themselves for these appropriate safeguards, but either necessity and proportionality tests, or data protection impact assessments (which include the afore-mentioned tests[32]) might be performed[33] or might be mandatory[34] in addition, with the aim of identifying more specific safeguards adapted to the situation and to the risks this situation generates.

4.1 Lawfulness as the need to identify a legal basis for processing

The GDPR and the national texts that implement Directive 2016/680 are the "natural" legal bases for data processing. Indeed, both the Regulation and the Directive have been adopted in order to authorise data processing under certain conditions that constitute safeguards ensuring the necessity and proportionality of processing operations. In this sense, both these texts constitute practical applications of the ECHR and EUCFR conditions that allow derogating from a fundamental right[35]:

- Directive 2016/680 applies 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

[32] See Article 35 of the GDPR.

[33] In relation to the scope of a DPIA, see Estelle De Marco, D2.10 - *Comparative study between the GDPR and Directive 95/46/EC including their relations to fundamental rights*, *op. cit.,* Section 2.4.1.2; Estelle De Marco, *Deliverable D2.4a (Intermediate) - Privacy Impact Assessment of the MANDOLA outcomes*, version 2.4a.2 of 11 July 2017, MANDOLA project (Monitoring ANd Detecting OnLine hAte speech) - GA n° JUST/2014/RRAC/AG/HATE/6652, http://mandola-project.eu/publications, Section 3.1.1.

[34] In relation to necessity and proportionality tests, see below the Sections 4.2.1.1.2 and 4.2.3.1 of the current guidelines. In relation to DPIA, see below the Section 5 of the current guidelines.

[35] See Estelle De Marco, D2.10 - *Comparative study between the GDPR and Directive 95/46/EC including their relations to fundamental rights*, *op. cit.*, Section 2.4.2.1.

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 leaflet are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

criminal penalties, including the safeguarding against and the prevention of threats to public security;[36]

- The GDPR applies to all other kind of processing, at the exclusion of those that take place by a natural person in the course of a purely personal activity, of those that fall outside the scope of the EU law (such as activities concerning national security[37]), and of those that fall within the scope of Chapter 2 of Title V of the TEU (relating to common foreign and security policies). Indeed, the first activity falls within the scope of the exercise of private life, the data controller's and the data subject's rights and obligations being both governed, in this situation, by the law protecting the exercise of private life[38], while the two last activities must be governed by specific legal basis providing for appropriate safeguards[39].

However, both Directive 2016/680 and the GDPR regulate most common data processing falling into their scope (in other words, data processing that

[36] Article 1 of Directive 2016/680; See also Bart Custers and Georgios Stathis, D2.2: *Review report on Directive 2016/680 aimed at the judiciary*, INFORM project (INtroduction of the data protection reFORM to the judicial system), JUST-JTRA-EJTR-AG-2016, GA n° 763866, http://informproject.eu/fr/resultats/, Chapter 2.

[37] See recital n° 16 of the GDPR.

[38] Privacy protection is generally covered by civil law at national levels, in addition to administrative or public law where the State is involved, national judges being entitled to apply the ECHR requirements for limiting freedoms: see for ex. Estelle De Marco in Estelle De Marco *et al.*, *MANDOLA Deliverable D2.2 - Identification and analysis of the legal and ethical framework*, version 2.2.4 of 12 July 2017, MANDOLA project (Monitoring ANd Detecting OnLine hAte speech) - GA n° JUST/2014/RRAC/AG/HATE/6652, http://mandola-project.eu/publications, Section 4.1.3 (introduction) and Section 4.1.3.1.

[39] The requirement to legally base any rights' limitation, including for national security purposes, has been recalled many times by the ECtHR, see for ex. case *Klass and others v. Germany*, appl. n° 5029/71, 6 September 1978, especially para. 49. This principle is also included partly in Article 23 of the GDPR (Restrictions).

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 leaflet are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

remain within certain limits in terms of impact on fundamental rights). Where processing operations are likely to present more risks for data subjects' fundamental rights than those that might generally be expected, and that, as a result, safeguards provided by Directive 2016/680 and the GDPR are not sufficient or are not suitable to frame these risks, both these latter texts require the adoption of a specific law that will provide in the particular situation for appropriate guarantees in order to ensure the necessity and the proportionality of processing operations[40]. For example, the GDPR requires the adoption of such specific legal basis in case personal data are processed for complying with a legal obligation or for the performance of a task carried out in the public interest (Article 6 para. 3)[41] or in case of derogations provided for by Article 23, or in order to authorise the processing of personal data related to criminal convictions or offences that will not be carried out under the control of official authority (Article 10). In the same line, the Directive requires for instance a specific legal authorisation for the processing of special categories of data (Article 10), for any exemption from the right to information of the data subject (Article 13 para. 3 and 4), and for processing, for the purposes of crime prevention or repression, data initially processed for other purposes (Article 4, para. 2).

[40] According to the Article 29 Data Protection Working Party "*a qualified test must be applied, to ensure that the legislative measure meets the criteria that allow derogating from a fundamental right. There are two aspects to this test: on the one hand the measure must be sufficiently clear and precise to be foreseeable, and on the other hand it must be necessary and proportionate, consistent with the requirements developed by the EUropean Court of Human Rights*": *Opinion 03/2013 on purpose limitation* (WP 203), 2 April 2013, p. 38; see also European Union Agency for Fundamental Rights and Council of Europe, *Handbook on European Data protection law*, December 2013, p. 64-66, http://www.echr.coe.int/Documents/Handbook_data_protection_ENG.pdf.

[41] See below, the Section 4.2.1.1.3 of the current guidelines.

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 leaflet are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

Where the legal basis is identified as being Directive 2016/680 or the Regulation, the principle of lawfulness implies further that the requirements of these texts, aiming to ensure the necessity and the proportionality of processing and the pursuit of a legitimate aim, are respected.

4.2 Lawfulness as the need to ensure the necessity and the proportionality of processing

In the Regulation as well in Directive 2016/680, several obligations ensure the necessity and the proportionality of processing as well as purpose legitimacy, beyond the obligations that are specifically studied in the other sections of the current guidelines (such as data subjects' rights and data controllers' obligations, especially in terms of accountability).

These obligations can be classified into five general categories which correspond to the requirements for legal grounds for processing, for legal grounds for processing special categories of data, for processing quality, for processing purposes quality, and for data qualities.

4.2.1 Legal grounds for processing

4.2.1.1 Legal grounds for processing in the GDPR

The GDPR provides for six possible "legal grounds" or "legal foundations" that might base processing operations. These foundations correspond actually to a list of purposes that are more specific than the "legitimate aim" required

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 leaflet are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

by the ECHR and the EUCFR[42], but that are broader than the "specific need" which must be identified during the necessity test to be performed under these instruments and which corresponds, in the GDPR and Directive 95/46/EC, to the specific purpose of processing[43]. These legal grounds are the following:

- **The consent of the data subject**

  To be noted that the consent of the data subject might be the unique and mandatory legal ground in certain cases, for example where traffic data are processed for marketing purposes or added value services[44]; where location data are used[45]; where are sent direct marketing communications[46]; or cookies or similar mechanisms[47]; and in many

[42] Estelle De Marco, D2.10 - *Comparative study between the GDPR and Directive 95/46/EC including their relations to fundamental rights*, March 2018, INFORM project (INtroduction of the data protection reFORM to the judicial system), JUST-JTRA-EJTR-AG-2016, GA n° 763866, http://informproject.eu/fr/resultats/, Sections 2.4.2.1 and 2.3.2.2.

[43] See below, n° 4.2.4 and Estelle De Marco, D2.10 - *Comparative study (between the GDPR and Directive 95/46/EC including their relations to fundamental rights)*, *op. cit.*, Section 2.3.2.3.1.

[44] Article 6, 3 of Directive 2002/58/EC, as modified by Directive 2009/136/EC.

[45] Article 9 of Directive 2002/58/EC. The definition of consent "*explicitly rules out consent being given as part of accepting the general terms and conditions for the electronic communications service offered*": Article 29 Data Protection Working Party, *Opinion on the use of location data with a view to providing value-added services* (WP 115), November 2005, p. 5.

[46] Article 13 of Directive 2002/58/EC, as modified by Directive 2009/136/EC. An exception does exist for communications related to products or services that are similar to the ones already sold to the customer.

[47] Article 5, 3 of Directive 2002/58/EC as modified by Directive 2009/136/EC. The practice which consists of informing the user in the website's general terms and conditions does not meet the requirements of the Directive, even if the browser is set to reject cookies, taking into account current browsers' functionalities: Article 29 Data Protection Working Party, *Opinion 2/2010 on online behavioural advertising* (WP 171), 22 June 2010, p. 13.

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 leaflet are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

situations of collection of special categories of data[48].

- **the performance of a contract** to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract[49];
- **compliance with a legal obligation** to which the controller is subject;
- **the protection of the vital interests** of the data subject or of another natural person;
- **the performance of a task carried out in the public interest** or in the exercise of official authority vested in the controller;
- **the legitimate interests pursued by the controller or by a third party**, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Four aspects of this list are particularly important and therefore imply a particular analysis: the definition of consent, the requirement to perform necessity and proportionality tests where another legal ground is chosen, the legal ground of compliance with a legal obligation to which the controller is subject; the legal ground of carrying out a task in the public interest and the legal ground of the legitimate interests pursued by the controller or by a third party.

---

[48] See below our Section 4.2.2. A separate opt-in consent is needed if data are collected through cookies: Article 29 Data Protection Working Party, *Opinion 2/2010 on online behavioural advertising*, *op. cit.*

[49] This legal ground is interpreted restrictively. To be used, personal data must be strictly necessary to the performance of the contract or to take steps prior to entering into a contract : see for ex. Article 29 data protection Working Party, *Guidelines on Consent under Regulation 2016/679* (WP259), 28 November 2017, Section 3.1.2, p. 9, 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 leaflet are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

4.2.1.1.1 The conditions for a valid consent

The consent of the data subject "*has always been a key notion in data protection*"[50], and for this reason a certain number of requirements must be respected in order to make it valid, the data controller having the obligation to be able to demonstrate[51] compliance with these requirements.

As stated in the GDPR[52] and recalled by the Article 29 Data protection working party[53] (becoming the European Data Protection Board in the GDPR[54]), a valid consent is a consent that corresponds to the following characteristics, keeping in mind that the GDPR adds additional requirements where consent is requested from a child in relation to information society services[55]:

- **Freely given:** this means that data subject must have a real choice to consent, without feeling compelled to consent or fearing negative consequences if they do not consent[56]. This implies four requirements:
    - Balance of power: the possibility for the data subject to choose and to control the situation must also be assessed in the light of the

[50] Article 29 data protection Working Party's *Opinion 15/2011 on the definition of consent* (WP187), p. 3 (Introduction).
[51] Article 29 data protection Working Party, *Guidelines on Consent under Regulation 2016/679* (WP259), 28 November 2017, Section 5.1, p. 19.
[52] Article 4 (11) of the GDPR.
[53] Article 29 data protection Working Party, *Guidelines on Consent under Regulation 2016/679* (WP259), 28 November 2017, p. 6.
[54] Article 68 of the GDPR.
[55] Article 29 data protection Working Party, *Guidelines on Consent under Regulation 2016/679* (WP259), *op. cit.*, Section 7, p. 23; Article 8 and Recital 38 of the GDPR.
[56] Article 29 data protection Working Party, *Guidelines on Consent under Regulation 2016/679* (WP259), *op. cit.*, Section 3.1.

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 leaflet are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

possible imbalance of powers between the data controller and the data subject. In this regard, public authorities[57] as well as employers[58] are considered to be often in a powerful position that prevent to consider the consent of the data subject as the most appropriate legal ground for processing (except where it is clear that the data subject have "*realistic alternatives to accepting the processing (terms) of the controller*" [59]).

- Absence of conditionality: in addition, a freely given consent is a consent that is not proposed as a condition for accessing a right or a service or good whereas the personal data processing is not necessary for the exercise of this right or the performance of a contract[60].
- Granularity: moreover, consent must be asked for each of the purposes that are pursued[61]. Where only one consent is requested in relation to several processing operations, it is presumed not to be freely given[62].
- Absence of detriment: refusing or withdrawing consent must be

[57] *Ibid.*, Section 3.1.1 p. 7.
[58] *Ibid.*, Section 3.1.1 p. 8.
[59] *Ibid.*, Section 3.1.1 p. 7.
[60] GDPR, Article 7, para. 4; Article 29 data protection Working Party, *Guidelines on Consent under Regulation 2016/679* (WP259), *op. cit.,* Section 3.1.2 p. 9.
[61] Article 29 data protection Working Party, *Guidelines on Consent under Regulation 2016/679* (WP259), *op. cit.,* Section 3.1.3, p. 11; Recital 32 of the GDPR.
[62] Article 29 data protection Working Party, *Guidelines on Consent under Regulation 2016/679* (WP259), 28 November 2017, Section 3.1.3, p. 11; Recital 43 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 leaflet are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission. [63]

possible "*without detriment*"[63]. In particular, no coercion, intimidation or "*significant negative consequences*"[64] must be feared in the absence of consent, and "*no clear disadvantage*" [65] must result from the withdrawal of a previously given consent.

- **Specific:** the consent must be given "*for one or more specific purposes*"[66]. This requirements "*aims to ensure a degree of user control and transparency for the data subject*"[67], and is closely linked both to the "granularity" requirement analysed above[68] and to the requirement of "informed" consent[69] analysed below.

  As a result, the specific nature of a consent requires together (1) the specification of the processing purposes, in sufficient detail to prevent function creep; (2) as many consent requests as there are distinct processing activities and (3) a clear separation of "*information related to obtaining consent for data processing activities from information about other matters*"[70].

[63] Article 29 data protection Working Party, *Guidelines on Consent under Regulation 2016/679* (WP259), *op. cit.*, Section 3.1.4, p. 11.
[64] *Ibid.*
[65] *Ibid.*
[66] Article 6 (1a) of the GDPR.
[67] Article 29 data protection Working Party, *Guidelines on Consent under Regulation 2016/679* (WP259), *op. cit.*, Section 3.2 p. 12.
[68] *Ibid.*, Section 3.1.3 p. 11.
[69] *Ibid.*, Section 3.2 p. 12.
[70] *Ibid.*, Section 3.2 p. 12.

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

- **Informed:** fair[71] and transparent[72] information must be provided to the data subject in relation to data processing operations, prior obtaining his or her consent. This "*is essential in order to enable* [data subjects] [...] *to make informed decisions*". As a result, in order to comply both with Article 6 and other provisions relating to fairness and transparency, the Article 29 data protection working party recommends to provide at least the following information (in order to ensure fairness), using clear and plain language, and therefore understandable for the "*average person*"[73] (in order to ensure transparency): (1) the controller's identity; (2) the purpose of each of the processing operations for which consent is sought; (3) what (type of) data will be collected and used; (4) the existence of the right to withdraw consent; (5) information about the use of the data for decisions based solely on automated processing, including profiling, in accordance with Article 22 (2)33; and (6) if the consent relates to transfers, about the possible risks of data transfers to third countries in the absence of an adequacy decision and appropriate safeguards[74].

[71] Art. 5 (1a) of the GDPR; Article 29 data protection Working Party, *Guidelines on Consent under Regulation 2016/679* (WP259), 28 November 2017, Section 3.3.1 p. 13; Estelle De Marco and Matthias Eichfeld, *Fundamental principles relating to processing of personal data*, INFORM project (INtroduction of the data protection reFORM to the judicial system), JUST-JTRA-EJTR-AG-2016, GA n° 763866, which can be found as Annex of several reports (included D2.10) published at http://informproject.eu/fr/resultats/, Section 1.2.

[72] Art. 5 (1a), Art. 7, Art. 12 and Recital 58 (see also Recitals 32, 39 and 60) of the GDPR; Article 29 data protection Working Party, *Guidelines on Consent under Regulation 2016/679* (WP259), *op. cit.*, Section 3.3.1 p. 13; Estelle De Marco and Matthias Eichfeld, *Fundamental principles relating to processing of personal data*, *op. cit.*, Section 1.3.

[73] Article 29 data protection Working Party, *Guidelines on Consent under Regulation 2016/679* (WP259), *op. cit.*, Section 3.3.2 p. 14.

[74] *Ibid.*, Section 3.4 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 leaflet are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

- **Unambiguous**: consent must be given unambiguously, *"by a statement or by a clear affirmative action* [by which the data subject], *signifies agreement to the processing of personal data relating to him or her*"[75].

  As a result, and without prejudice to national contract law, "*consent can be collected through a written or (a recorded) oral statement, including by electronic means*"[76], but the "*use of pre-ticked opt-in boxes*"[77], "*silence or inactivity* [...] *as well as merely proceeding with a service cannot be regarded as an active indication of choice*"[78]. Neither can be seen as a valid consent the "*blanket acceptance of general terms and conditions*" [79] or "*opt-out constructions that require an intervention from the data subject to prevent agreement*" [80].

4.2.1.1.2 The requirement to perform necessity and proportionality tests under the other legal grounds

Where the identified legal ground for processing is not the consent of the data subject, processing operations must be "necessary" to fulfil the purpose mentioned in one of the other possible legal grounds[81], and the data controller must be able to demonstrate[82] such a necessity.

---

[75] Article 4 (11) of the GDPR ; Article 29 data protection Working Party, *Guidelines on Consent under Regulation 2016/679* (WP259), 28 November 2017, Section 3.3.1 p. 13.
[76] Article 29 data protection Working Party, *Guidelines on Consent under Regulation 2016/679* (WP259), *op. cit.*, Section 3.4 p. 16.
[77] *Ibid.*
[78] *Ibid.*
[79] *Ibid.*
[80] *Ibid.* p. 17.
[81] See Article 6 of the GDPR.
[82] Article 29 data protection Working Party, *Guidelines on Consent under Regulation 2016/679* (WP259), 28 November 2017, Section 5.1, p. 19.

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

This term must be understood as having the same meaning of the formula "*necessary in a democratic country*" of the ECHR, which includes the principles of necessity and proportionality[83], and of the term "necessary" used in article 52, 1 of the EUCFR.[84] In this regard, as it has been highlighted by the Article 29 Data Protection Working Party, "*the term 'necessary' in the* [...] [legislation] *provides an important safeguard in relation to legitimacy of processing of personal data*"[85].

Therefore, the data controller must **determine whether the processing operations are "necessary"** to pursue the processing purposes, through the performance of a necessary and proportionality test as described in Sections 2.3.2.3 and 2.3.2.4 of the Comparative study between the GDPR and Directive 95/46/EC including their relations to fundamental rights performed under the INFORM project[86]. This test *inter alia* implies to assess whether "*there are other less invasive means to reach the identified purpose*"[87].

[83] See Estelle De Marco, D2.10 - *Comparative study between the GDPR and Directive 95/46/EC including their relations to fundamental rights*, March 2018, INFORM project (INtroduction of the data protection reFORM to the judicial system), JUST-JTRA-EJTR-AG-2016, GA n° 763866, http://informproject.eu/fr/resultats/, Section 2.3.2.

[84] *Ibid.*, Section 2.3.1, para. 2.

[85] Article 29 Data Protection Working Party, *Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector* (WP 211), *27 February 2014,* Section 4.2.

[86] Estelle De Marco, D2.10 - *Comparative study between the GDPR and Directive 95/46/EC including their relations to fundamental rights*, March 2018, INFORM project (INtroduction of the data protection reFORM to the judicial system), JUST-JTRA-EJTR-AG-2016, GA n° 763866, http://informproject.eu/fr/resultats/

[87] Article 29 Data Protection Working Party's *Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC* (WP 217), 9 April 2014, Annex 1 p. 55 (see also n°II.3, p. 11 and III.3.1, p. 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 leaflet are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

4.2.1.1.3 The legal grounds of compliance with a legal obligation to which the controller is subject, and of carrying out a task in the public interest

These legal grounds are the two main ones that are appropriate to base processing operations performed by the judiciary[88].

However, both can only base a personal data processing where a specific EU law or national law - which will come in addition to a possible national law dedicated to the correct application of the GDPR) authorises such processing. As analysed in the Section 4.1 of the current guidelines, such a specific law must provide for appropriate guarantees in order to ensure the necessity and the proportionality of processing operations. In this regard, Article 6 para. 3 of the GDPR[89] clarifies that this law must meet an objective of public interest, and must specify the purposes of the processing, as well as specific guarantees in case of derogations from the GDPR, such as "*the general conditions governing the lawfulness of processing by the controller; the types of data which are subject to the processing; the data subjects concerned; the entities to, and the purposes for which, the personal data may be disclosed; the purpose limitation; storage periods; and processing operations and processing procedures, including measures to ensure lawful and fair processing such as those for other specific processing situations as provided for in Chapter IX*" of the GDPR.

[88] Article 29 data protection Working Party, *Guidelines on Consent under Regulation 2016/679* (WP259), 28 November 2017, Section 3.3.1 p. 7; footnote n°15.
[89] See also Recital 45 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 leaflet are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

4.2.1.1.4 The legal ground of the legitimate interests pursued by the controller or by a third party

This legal ground cannot, *a priori*, be used by the judiciary to base personal data processing since it must "*not apply to processing carried out by public authorities in the performance of their tasks*"[90]. However, it is important to understand its meaning in view of trials related to the compliance with the GDPR of processing operations carried out by other data controllers.

In order use this legal ground[91], a "test of legitimate interest" must be performed, and in this regards the guidelines from the Article 29 Working Party and from Recital 47 of the GDPR must be followed.

The Article 29 Data Protection Working Party clarified that, in order to comply with legal requirements, a legitimate interest must be "*lawful (i.e. in accordance with applicable EU and national law)*", must "*represent a real and present interest (i.e. not be speculative)*", and must "*be sufficiently clearly articulated*" (i.e. "*sufficiently specific*" or "*concrete*"[92]), to allow "*a balancing test to be carried out against the interest and fundamental rights of the data subject*"[93]. This analysis has been done

[90] Art. 6 para. 1 last indent of the GDPR.
[91] Some elements of this Section have been already published by the author of the current Section 4 in Estelle De Marco *et al.*, *MANDOLA Deliverable D2.2 - Identification and analysis of the legal and ethical framework*, version 2.2.4 of 12 July 2017, MANDOLA project (Monitoring ANd Detecting OnLine hAte speech) - GA n° JUST/2014/RRAC/AG/HATE/6652, http://mandola-project.eu/publications, Section 4.2.3.3.6.
[92] Article 29 Data Protection Working Party, *Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC* (WP 217), 9 April 2014, III.3.1, p. 23 and Annex 1, p. 55.
[93] *Ibid.*, III.3.1, p. 25.

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

under Directive 95/46/EC, but it can be equally applied under the GDPR since the rule stays the same[94].

To conduct this test, the Article 29 Data Protection Working Party advises to consider several factors by following a series of steps:

- **Assessment of the controller's or other party's legitimate interest:** "*the nature of the interests*" of the data controller or of the other party must be identified (fundamental right, other personal, public or collective interest), as well as "*the possible prejudice suffered by the controller, by third parties or the broader community if the data processing does not take place*"[95].

- **Assessment of the impact on the data subjects:** this step implies to identify[96]:
  - ✓ "*the nature of the data*" that will be processed;
  - ✓ the "*status of the data subject and (…) of the controller*", which means among other identifying their potential dominant position or weaknesses;
  - ✓ the way the data will be processed and the scale of the processing operations;

[94] Article 29 data protection Working Party, *Opinion 2/2017 on data processing at work* (WP 249), 8 June 2017, Section 6.2, p. 23; *Guidelines on Consent under Regulation 2016/679* (WP259), 28 November 2017, Section 3.1.1, p. 6.
[95] Article 29 Data Protection Working Party, *Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC* (WP 217), *op. cit.*, Annex 1 p. 55.
[96] All quotations are coming from Article 29 Data Protection Working Party, *Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC* (WP 217), *op. cit.*, Annex 1 p. 55 and 56.

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 leaflet are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

- ✓ "*the fundamental rights and/or interests of the data subjects that could be impacted*";
- ✓ *the "data subjects' reasonable expectations",* and
- ✓ *the "impacts on the data subject",* which must be compared *"with the benefit expected from the processing by the data controller".*

- **Establishing a provisional balance:** the outcomes of the previous steps must be balanced, taking also into account the measures taken by the data controller to comply with the other requirements of the GDPR.

- **Implementing additional safeguards and establishing a final balance:** a final balance between the rights and interests at stake must be established, taking into account the additional safeguards that the controller decides to implement, to reduce or eliminate the weaknesses found out during the previous steps (collection of less data, short term deletion, functional separation, "*extensive use of anonymisation techniques*", "*increased transparency*", "*privacy enhancing technologies, privacy by design, privacy and data protection impact assessments*", etc.)[97].

- **Establishing and communicating proofs of compliance:** the current assessment should be documented, the documentation should be kept available to the relevant data protection authorities and its outcomes should be communicated to data subjects. However, the Article 29 Data Protection Working Party adds that the "***details of assessment and documentation*" must be adapted to the envisaged processing**

[97] Article 29 Data Protection Working Party, *Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC* (WP 217), 9 April 2014, III.3.4, p. 42, see also Annex 1 p. 56.

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 leaflet are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

operations, and to the risks they create to the rights of data subjects. This compliance test may for instance become a "*key part*" of a broader privacy impact assessment when "*a processing operation presents specific risks to the rights and freedoms of the data subjects*"[98].

As already explained, this balancing test stays applicable within the framework of the GDPR, which in addition emphasises the special care to be taken where the processing involves children's personal data[99].

The performance of this test is particularly important for employers who base on the ground of their legitimate interest the processing of employees' personal data. Indeed, in this situation, "*it is essential that specific mitigating measures are present to ensure a proper balance between the legitimate interest of the employer and the fundamental rights and freedoms of the employees*"[100]. In this regard, the Article 29 working party provides for additional advises in relation to several scenarios "*in which new technologies and/or developments of existing technologies have, or may have, the potential to result in high risks to the privacy of employees*"[101]: processing operations during the recruitment process, processing operations resulting from in-employment screening, processing operations resulting from in-employment screening, processing operations resulting from monitoring ICT usage at the workplace, processing operations resulting from monitoring ICT usage outside the workplace, processing operations relating to time and

[98] *Ibid.*, Annex 1 p. 56.
[99] Article 6 (f) of the GDPR.
[100] Article 29 data protection Working Party, *Opinion 2/2017 on data processing at work* (WP 249), 8 June 2017, Section 6.2, p. 23; *Guidelines on Consent under Regulation 2016/679* (WP259), 28 November 2017, p. 7 (last indent).
[101] Article 29 data protection Working Party, *Opinion 2/2017 on data processing at work* (WP 249), *op. cit.*, Section 5, 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 leaflet are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

attendance, processing operations using video monitoring systems, processing operations involving vehicles used by employees, processing operations involving disclosure of employee data to third parties and processing operations involving international transfers of HR and other employee data[102].

4.2.1.2 Legal grounds for processing in Directive 2016/680

In relation to 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*"[103], the relevant national law that transposes Directive 2016/680 is applicable as a special law instead of the GDPR.

> However, as it is recalled in the Section 2.3 of the current guidelines and in Article 9 of the Directive, it is to be noted that further processing for other purposes fall under the GDPR requirements, and must be authorised by a specific law (unless they fall outside the scope of the EU law, and in this situation the principles of legal basis, necessity and proportionality must be ensured based on the ECHR and EUCFR requirements[104]).

Directive 2016/680 does provide for one legal ground only considering the nature of the processing activities.

Indeed, Article 8 of the Directive states that processing operations are "*lawful only if and to the extent that processing is necessary for the performance of a task carried*

[102] *Ibid*, p. 11 *et seq*.
[103] Article 1 para. 1 of Directive 2016/680.
[104] See above the Section 4.1 of the current guidelines.

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 leaflet are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

out by a competent authority for the purposes" of crime repression or prevention as formulated in the introduction of the current Section "*and that it is based on Union or Member State law*", which means that processing operations must be authorised by the national law that transposes the Directive or another relevant specific law. This law must at least specify "*the objectives of processing, the personal data to be processed and the purposes of the processing*"[105], and of course any guarantee of necessity and proportionality that would not be provided for in the text that implements Directive 2016/680[106].

4.2.2 Legal grounds for processing special categories of data

4.2.2.1 Legal grounds for processing special categories of data in the GDPR

Processing operations that relate to special categories of data as defined by law must, in addition to be based on one of the legal grounds listed in Article 6 of the GDPR, be based on one of the grounds that are listed in Article 9 of the GDPR.

Special categories of data are personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership; genetic data, biometric data where the purpose is to uniquely identify a natural person; data concerning health; and data concerning a natural person's sex life or sexual orientation.

[105] Article 9 of Directive 2016/680.

[106] See above, the Section 4.1 of the current guidelines.

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 leaflet are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

In order to process such kind of data, the data controller must be able to demonstrate[107] one of the following situations:

- "*The data subject has given explicit consent to the processing of those personal data for one or more specified purposes",* except where the EU or the relevant national law prohibits the processing of the intended data.

  The conditions analysed in the Section 4.2.1.1.1 of the current guidelines are applicable to the validity of the consent of the data subject under Article 9 of the GDPR.

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

  This legal ground might be used by the judiciary where it acts as an employer.

- "*Processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent*".

  This legal ground might be applicable to judges or prosecutors in countries where one of their missions might be to take decisions to protect the vital interests of natural persons who cannot consent.

[107] Article 29 data protection Working Party, *Guidelines on Consent under Regulation 2016/679* (WP259), 28 November 2017, Section 5.1, p. 19.

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

- "*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*".

  This legal ground is not applicable to the judiciary, but judges might have to analyse if it has been properly applied by other data controllers.

- "*Processing relates to personal data which are manifestly made public by the data subject*".

  This legal ground might be applicable to personal data processed by the judiciary. However, two crucial elements should be kept in mind:

  - The principle of fairness[108] implies that the data subject "*was aware that the respective data will be publicly available*". In case of doubt, "*a narrow interpretation should be applied*"[109].
  - The public nature of the personal data does not exempt from respecting the other provisions of the GDPR, which means that where this legal ground is used, a compatibility test must be

[108] To draw an analogy with cases where the consent of the data subject is a legal ground: see Article 29 data protection working party, *Opinion 15/2011 on the definition of consent* (WP 187), 13 July 2011, p. 9, para. 1.

[109] Article 29 data protection working party, *Opinion on some key issues of the Law Enforcement Directive (EU 2016/680)* (WP 258), 29 November 2017, pp. 10 and 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 leaflet are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

performed[110], as an application of the principle of purpose limitation[111].

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

  As highlighted in the *Guidelines on GDPR and Directive 2016/680 aimed at court staff* produced under the INFORM project, this legal ground might be used by the judiciary in order to base processing of personal data, but "*the scope of judicial capacity exception should apply only to adequate processing of special categories of personal data relevant to the court proceeding or other court activity with the sensitivity of such personal data being taken into consideration*".[112]

- "*Processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject*".

  This legal ground might be applicable to personal data processed by the judiciary, provided that a law authorises the processing operations and frames the latter with appropriate safeguards.

- "*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*

[110] Article 29 data protection Working Party, *Opinion 03/2013 on purpose limitation*, (WP 203), p. 14 footnote 31; Section III.2.5 p. 35 last para., and Annex 2.
[111] See below, the Section 4.2.4 of the current guidelines.
[112] eLAW *et al.*, *Guidelines on GDPR and Directive 2016/680 aimed at court staff*, INFORM project (INtroduction of the data protection reFORM to the judicial system), JUST-JTRA-EJTR-AG-2016, GA n° 763866, http://informproject.eu/fr/resultats/, Section 4.2, referring to Boris P Paal and others, Datenschutz-Grundverordnung: DS-GVO (C.H.Beck 2017), Art. 9, Rn. 37.

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

health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3".

This legal ground is not applicable to the judiciary, but judges might have to analyse if it has been properly applied by other data controllers. To be noted that this legal ground can be used only where data are processed "*by or under the responsibility of a professional subject to the obligation of professional secrecy under Union or Member State law or rules established by national competent bodies or by another person also subject to an obligation of secrecy under Union or Member State law or rules established by national competent bodies*"[113].

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

  This legal ground is not applicable to the judiciary, but judges might have to analyse if it has been properly applied by other data controllers.

- "*Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued,*

[113] Article 9, para.3 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 leaflet are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject".

This legal ground might be applicable to personal data processed by the judiciary, provided that a law authorises the processing operations and frames the latter with appropriate safeguards.

4.2.2.2 Legal grounds for processing special categories of data in Directive 2016/680

Under Directive 2016/680, processing of special categories of personal data (as they have been defined in the previous Section) is only possible:

(1) where it is "*strictly necessary*", subject "*to appropriate safeguards for the rights and freedoms of the data subject*", and

(2) where it is authorised by the EU or the relevant member State's law, either "*to protect the vital interests of the data subject or of another natural person*", or "*where such processing relates to data which are manifestly made public by the data subject*"[114].

The formula "*strictly necessary*" must be understood, according to the Article 29 data protection working party, "*as a call to pay particular attention to the necessity principle in the context of processing special categories of data, as well as to foresee precise and particularly solid justifications for the processing of such data*"[115]. In this regards, the Working party recommends that in such situations, "*the competent authorities are committed to carrying out a data protection impact assessment (DPIA)*"[116], which

[114] Article 10 of Directive 2016/680.
[115] Article 29 data protection working party, *Opinion on some key issues of the Law Enforcement Directive (EU 2016/680)* (WP 258), 29 November 2017, p.8.
[116] *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 leaflet are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

should assess and demonstrate "*whether the purpose of the processing (e.g. criminal investigation) cannot be achieved by processing which affects the rights and freedoms of the data subject less and if the processing of special categories of data does not represent a risk of discrimination for the data subject*" [117].

In addition, appropriate safeguards (in other words safeguards that are sufficient to protect individuals against risks) must be foreseen and implemented[118].

Moreover, a law must authorise the processing operations, either based on the consent of the data subject, and/or based on the public nature of processed personal data.

- In case of consent, this consent of the data subject should only be considered within the boundaries allowed by the legislator for special categories of data[119].
- In case processed personal have been made public, the data controller should be able to demonstrate that the data subject "*was aware that the respective data will be publicly available which means to everyone including authorities* [and] *in case of doubt, a narrow interpretation should be applied*"[120].

[117] *Ibid.*
[118] *Ibid.* See also Recital 37 of Directive 2016/680.
[119] Article 29 data protection working party, *Opinion on some key issues of the Law Enforcement Directive (EU 2016/680)* (WP 258), 29 November 2017, pp.9 and 10.
[120] *Ibid.,* pp. 10 and 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 leaflet are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

4.2.3 Quality of processing

Processing operations must comply with three principles which are the principles of fairness, of lawfulness and of transparency[121].

4.2.3.1 The principle of lawfulness

As it has already been highlighted previously in the current guidelines, the principle of lawfulness refers to the compliance with law in a broad sense, which implies that processing operations:

- Are authorised by a clear, specific, accessible and foreseeable legal basis, which might be the GDPR, the law that implements Directive 2016/680, or another applicable law[122];
- Are based on one of the legal grounds listed in Article 6 of the GDPR or in Article 9 of Directive 2016/680[123];
- Are based in addition, where special categories of data are processed, on one of the legal grounds listed in Article 9 of the GDPR or in Article 10 of Directive 2016/680[124];
- Comply with the other requirements of the applicable law[125], which might themselves require additional necessity and proportionality tests in order to identify safeguards that would be specifically needed in the particular

[121] Article 5 (1a) of the GDPR; Article 4 (1a) and Recital 26 of Directive 2016/680.
[122] See the introduction of Section 4 and Section 4.1 of the current guidelines.
[123] See the Section 4.2.1 of the current guidelines.
[124] See the Section 4.2.2 of the current guidelines.
[125] See the introduction of Section 4 of the current guidelines.

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 leaflet are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

situation. It is for example the case in Article 6[126], 23 and 35 of the GDPR.

To be noted that the Article 29 data protection working party has also recalled that in a series of "*data processing at work scenarios in which new technologies and/or developments of existing technologies have, or may have, the potential to result in high risks to the privacy of employees*"[127], employers "*should consider whether* [...] *the processing activity is necessary, and if so, the legal grounds that apply*"[128], and whether "*the processing activity is proportionate to the concerns raised*"[129]. The working party adds the requirements of verifying the fairness and the transparency of processing operations, which are also requirements that ensure proportionality[130].

4.2.3.2 The principle of fairness

The principle of fairness (Article 5a of the GDPR and article 4 of Directive 2016/680) refers to the prohibition of secrecy and to the requirement of comprehensive information[131]. In particular, natural persons should be made

[126] See above the Section 4.2.1.1.2 of the current guidelines.
[127] Article 29 data protection Working Party, *Opinion 2/2017 on data processing at work* (WP 249), 8 June 2017, Section 5, p. 10.
[128] *Ibid.*, Section 5, p. 11.
[129] *Ibid.*, Section 5, p. 12.
[130] Estelle De Marco, D2.10 - *Comparative study between the GDPR and Directive 95/46/EC including their relations to fundamental rights*, March 2018, INFORM project (INtroduction of the data protection reFORM to the judicial system), JUST-JTRA-EJTR-AG-2016, GA n° 763866, http://informproject.eu/fr/resultats/, Section 2.3.2.4.2.
[131] See Estelle De Marco and Matthias Eichfeld, *Fundamental principles relating to processing of personal data*, INFORM project (INtroduction of the data protection reFORM to the judicial system), JUST-JTRA-EJTR-AG-2016, GA n° 763866, which can be found as Annex of several reports (included D2.10) at

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 leaflet are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

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[132] such as, for processing operations falling into the scope of the GDPR, the specific context and circumstances of these processing operations, and the question of whether personal data are mandatory and incurred consequences in case of silence[133]. In essence, the principle of fairness 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[134].

Naturally, fairness does not imply to provide for information that would be detrimental to the legitimate aim pursued. As a result, the information to be provided to data subjects under the Directive might be restricted by the national law in relation to particular data processing operations, in the pursuit of purposes falling into a restrictive list provided for in Article 13 (3) of the Directive. However, this limitation is only allowed "*to the extent that it is necessary and proportionate in order to avoid any of the prejudices outlined in Article 13(3). Any*

http://informproject.eu/fr/resultats/, Section 1.2; Recital 38 to Directive 95/46/EC. See also Judgement of the CJEU, 1 October 2015, C-201/14 (case "Smaranda Bara"), para. 34.

[132] See Recitals 39 and 60 of the GDPR; Recitals 26 and 42 of Directive 2016/680.

[133] See Recital 60 of the GDPR.

[134] Most of the content of this paragraph comes from Estelle De Marco and Matthias Eichfeld, *Fundamental principles relating to processing of personal data*, *op. cit.*, Section 1.2.

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

legislative measures must have due regard to the fundamental rights and the legitimate interests of the data subject"[135].

4.2.3.3 The principle of transparency

4.2.3.3.1 The principle of transparency under the GDPR

The principle of transparency contributes to the quality of the information to be provided to data subjects, both in terms of form and in terms of content.

Indeed, the principle of transparency[136] adds first, to the requirement of fairness or in other words of completeness of the information to be provided, a requirement of clarity of this information.

Transparency means therefore firstly, under the GDPR, to provide the necessary information (which means the "fair" information[137]) "*in a concise, transparent, intelligible and easily accessible form, using clear and plain language*" [138].

Therefore, the latter requirement is a requirement of form. It applies to all the information that must be provided, in order to ensure a fair and transparent processing[139]. It enables *inter alia* to reinforce the obligation of the data controllers to clearly indicate to data subjects which data are required and

[135] Article 29 data protection working party, *Opinion on some key issues of the Law Enforcement Directive (EU 2016/680)* (WP 258), 29 November 2017, p 18.
[136] A large part of the content of the current Section 4.2.3.3 comes from Estelle De Marco and Matthias Eichfeld, *Fundamental principles relating to processing of personal data*, *op. cit.*, Section 1.3.
[137] See above the Section 4.2.3.2 of the current guidelines.
[138] Article 12 (1) of the GDPR. See also Recitals 39 and 58 of the GDPR.
[139] See Recital 58 p. 1 and Recital 39 p. 2. See also Art. 12 para. 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 leaflet are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

which are not in the light of the purposes that are pursued, among the data that are requested[140].

Secondly, transparency appears as an extension of both the principle of fairness and the obligation of data subject's information, in order to command to inform data subjects about all aspects of the data processing which transparency is likely to ensure fairness. This leads to ensure fairness in the broadest possible way instead of ensuring it in a minimalist way.

As a result, the principles of fairness and transparency concern together both the method and the content of the information[141], the principle of transparency contributing to both content and form.

The implementation of transparency as a new independent principle 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[142].

---

[140] See Recital n°43 of the GDPR: « *Consent is presumed not to be freely given if it does not allow separate consent to be given to different personal data processing operations despite it being appropriate in the individual case, or if the performance of a contract, including the provision of a service, is dependent on the consent despite such consent not being necessary for such performance*". See also Recital n° 60 of the GDPR and its Article 7 that regulates the conditions for data subject's consent. See also Estelle De Marco, D2.10 - *Comparative study between the GDPR and Directive 95/46/EC including their relations to fundamental rights*, March 2018, INFORM project (INtroduction of the data protection reFORM to the judicial system), JUST-JTRA-EJTR-AG-2016, GA n° 763866, http://informproject.eu/fr/resultats/, Section 3.3.1.

[141] 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.

[142] See Art. 29 Data Protection Working Party, *Guidelines on transparency under Regulation 679/2016* (WP 260), p. 5; see also Commission Staff Working Paper SEC (2012)72 final, Annex 2, Section. 2.4, available

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 leaflet are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

This principle of transparency is new in the GDPR but it was already latent in Directive 95/46/EC, along with the concept of predictability[143] (which has for its part not been included in the GDPR even though foreseeability is evoked in Recital n°41 of the latter)[144], both on the basis of the ECHR and EUCFR principles[145] and on the basis of the analysis of the Article 29 Working party[146]. For example, the latter working party considered under Directive 95/46/EC that the requirement for transparency at work implies, based on Articles 10 and 11 of the Directive, that employees are "*informed of the existence of any monitoring, [of] the purposes for which personal data are to be processed and [of] any other information necessary to guarantee fair processing*"[147], the need for transparency becoming "*more evident*" [148] within the framework of the use of new technologies since the latter "*enable the collection and further processing of possibly huge amounts of personal data in a covert way*"[149].

4.2.3.3.2 The principle of transparency under Directive 2016/680

Whereas the obligation of transparency is clearly stated in Article 5a of the GDPR, it disappears from the text of Directive 2016/680. It stays only

at http://ec.europa.eu/justice/data-protection/document/review2012/sec_2012_72_annexes_en.pdf.

[143] Article 29 Data Protection Working Party, *Opinion 03/2013 on purpose limitation*, 2 April 2013, WP203, Section II.3 p.13.

[144] See Estelle De Marco, D2.10 - *Comparative study between the GDPR and Directive 95/46/EC including their relations to fundamental rights*, *op. cit.*, Section 3.3.1.

[145] *Ibid.*, Sections 2.3.2.1.1 and 2.3.2.4.2.

[146] See for ex. Article 29 Data Protection Working Party, *Opinion 03/2013 on purpose limitation*, 2 April 2013, WP203, Sections II.3 p. 13; II.1.2 p. 18.

[147] Article 29 data protection Working Party, *Opinion 2/2017 on data processing at work* (WP 249), 8 June 2017, Section 3.1.2, p. 8.

[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 leaflet are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

mentioned in Recital 26 of the Directive, and Article 12 (1) of the Directive clarifies that any communication to the data subject must be "*concise, intelligible and easily accessible form, using clear and plain language*". The latter wording is therefore exactly the same as the one used in the GDPR in relation to the requirement of transparency of the information in terms of form, at the exception of the word "transparency" itself, which has been removed.

This might be due to the fact that processing data for the purpose of crime prevention or repression might command in certain cases to hide some information whose disclosure would be prejudicial to the aim pursued[150], while the word "transparency", as we analysed it in the previous Section, contains the idea of "saying everything" beyond its role in terms of intellectual accessibility.

This removal is regrettable since the principle of transparency - to the extent it relates to the form of the information-, as long as the principle of fairness, apply to police and judiciary processing operations, keeping in mind that the delay, restriction or omission of the provision to data subjects of the information listed in Article 13 (1 and 2) of Directive 2016/680 can only be authorised by law "*to the extent that, and for as long as, such a measure constitutes a necessary and proportionate measure in a democratic society with due regard for the fundamental rights and the legitimate interests of the natural person concerned, in order to*" safeguard one of the interests restrictively listed in Article 13 (3). In addition, transparency is an ECHR and EUCFR requirement[151] that also applies to

[150] Article 13 (3) of Directive 2016/680; Section 4.2.3.2 (last para.) of the current guidelines.
[151] See below the Section 4.2.3.3.1 of the current guidelines.

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 leaflet are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

LEA and courts processing operations, which is confirmed in Recital 26 of Directive 2016/680.

As a result, the principle of transparency applies to processing operations by competent authorities for the purposes of crime prevention and repression, with possible legal, necessary and proportionate exceptions where the information could prejudice to the legitimate aim pursued, affecting therefore transparency in terms of the content of the information to be provided.

4.2.4 Quality of processing purposes

4.2.4.1 Presentation and importance of the quality of processing purposes

According to Article 5 (b) of the GDPR, the purposes of processing operations must be specified, explicit and legitimate. In addition, "*once data are collected, they must not be further processed in a way incompatible with those purposes*"[152], and any reuse without the consent of the data subject or a specific legal authorisation requires the performance of a compatibility test which content is provided for in Article 6 (4) of the GDPR, whether or not new processing activities have or not the same purposes[153].

These principles of specified, explicit, legitimate purposes and of compatibility of processing with purposes (including the non-diversion of

[152] Article 29 Data Protection Working Party, *Opinion 03/2013 on purpose limitation*, 2 April 2013, WP203, p. 4.

[153] Even this is not specified in the GDPR, this is the opinion of the Article 29 data protection working party based on Article 6 (1b) of Directive 95/46/EC (which wording is the same as in Article 5 (1b) of the GDPR). Indeed, these provisions contain the formula "*not processed in a manner that is incompatible with those purposes*", which does not impose that purposes are modified within the framework of the new processing: Article 29 data protection working party *Opinion 03/2013 on purpose limitation*, 2 April 2013, WP203, Section III.2.1.

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 leaflet are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

these purposes) are "*a prerequisite for applying other data quality requirements* [...] [since they] *contribute to transparency, legal certainty and predictability in the exact same way*"[154].

As a result, these principles were already included in Directive 95/46/EC[155], the purposes to be specified corresponding in addition to the need that must be identified during the course of an ECHR and EUCFR necessity test[156]. The content of the compatibility test provided for in the GDPR is also a faithful copy of the one proposed under Directive 95/46/EC by the Article 29 data protection working party[157]. Indeed, the GDPR evokes explicitly the same steps and concludes identically on the conditions under which further processing for historical, statistical or scientific purposes is not considered as incompatible[158], such an exception being also embodied by the GDPR (which adds the purposes of archiving in the public interest and which regulates this exception in more details - following partly the Article 29 working group - in its Article 89).

As regards Directive 2016/680, the principles are also the same, at the exception of the requirement to perform a compatibility test, which is not

---

154 Article 29 Data Protection Working Party, *Opinion 03/2013 on purpose limitation*, *op. cit.*, Section II.2 p.11.

155 Article 6 (b) of Directive 95/46/EC.

156 *Article 29 Data Protection Working Party, Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector (WP 211)*, 3.13; See also Estelle De Marco, D2.10 - *Comparative study between the GDPR and Directive 95/46/EC including their relations to fundamental rights*, March 2018, INFORM project (INtroduction of the data protection reFORM to the judicial system), JUST-JTRA-EJTR-AG-2016, GA n° 763866, http://informproject.eu/fr/resultats/, Sections 3.3.2 and 2.3.2.3.1.

157 Article 29 Data Protection Working Party, *Opinion 03/2013 on purpose limitation*, *op. cit.*, Section III.2 pp. 20 *et seq*.

158 *Ibid.*, Section III.2.3 p. 28.

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

mentioned. Indeed, in the Directive, the reuse of data for a purpose other than the purpose for which the personal data are collected must be authorised by a law ensuring necessity and proportionality[159]. However, the compatibility test as it has been advised by the Article 29 data protection working party stays mandatory in relation to the general obligation of compatibility of the processing with purposes[160], in a reading of the Directive that is in line with the fundamental objectives and with the spirit of the data protection legislation. In addition, under a similar approach, a compatibility test should be required in order to identify the appropriate safeguards to be provided for in the law that will authorise purpose diversion.

4.2.4.2 Content of the principles of specified, explicit, legitimate and non-diverted purposes

- "Specified purposes" means that "*- prior to, and in any event, no later than the time when the collection of personal data occurs - the purposes must be precisely and fully identified to determine what processing is and is not included within the specified purpose and to allow that compliance with the law can be assessed and data protection safeguards can be applied*"[161].
- "Explicit purposes" means that "*purposes must be explicit, that is, clearly revealed, explained or expressed in some form in order to make sure that everyone*

[159] Articles 4 (2) and 9 (1) of Directive 2016/680.
[160] Indeed, Article 4 (1b) of Directive 2016/680 uses the same formula as Article 5 (1b) of the GDPR (and as Article 6 (1b) of Directive 95/46/EC).
[161] Article 29 Data Protection Working Party, *Opinion 03/2013 on purpose limitation*, 2 April 2013, WP203, p. 39. For further details see Estelle De Marco and Matthias Eichfeld, *Fundamental principles relating to processing of personal data*, INFORM project (INtroduction of the data protection reFORM to the judicial system), JUST-JTRA-EJTR-AG-2016, GA n° 763866, which can be found as Annex of several reports (included D2.10) at http://informproject.eu/fr/resultats/, Section 2.1.

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 leaflet are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

concerned has the same unambiguous understanding of the purposes of the processing irrespective of any cultural or linguistic diversity. Purposes may be made explicit in different ways"[162]. Where purposes have not been specified adequately by the data controller, "*all the facts should be taken into account to determine the actual purposes, along with the common understanding and reasonable expectations of the data subjects based on the context of the case*" [163].

- "Legitimate purposes" means "*that the purposes must be 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*".

- The compatibility test, to be performed in case the data controller is willing to process personal data in a way that has not been specified at the time of the original data collection (whether or not new processing activities have or not the same purposes[164]), must include the following steps:[165]

---

[162] Article 29 Data Protection Working Party, *Opinion 03/2013, op. cit.,* p. 39. For further details see Estelle De Marco and Matthias Eichfeld, *Fundamental principles relating to processing of personal data*, *op. cit.*, Section 2.2.

[163] Article 29 Data Protection Working Party, *Opinion 03/2013, op. cit.,* p. 20. For further details see Estelle De Marco and Matthias Eichfeld, *Fundamental principles relating to processing of personal data*, *op. cit.*, Section 2.3.

[164] See above, the Section 4.2.1.4, para. 1. of the current guidelines.

[165] For further explanations see Estelle De Marco *in Estelle De Marco et al.*, *MANDOLA Deliverable D2.2 - Identification and analysis of the legal and ethical framework*, version 2.2.4 of 12 July 2017, MANDOLA project (Monitoring ANd Detecting OnLine hAte speech) - GA n°

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

- Identification of both the new and the original purpose;
- Identification of the "substance" of the relationship between these two purposes to determine if the first one was already implied in the second one;
- Appreciation of the reasonable expectations of privacy of the data subject in the specific context, including with regard to his or her freedom of choice to give his or her data;
- Assessment of the data sensitivity and of the impact of the further processing on individuals, including emotional impacts; and
- Identification of the safeguards that are suitable to compensate the weaknesses identified during the previous tests and to prevent any undue impact on the data subjects. Some of these safeguards may consist in technical and organisational measures ensuring functional separation, particularly important in a big data context (measures ensuring that the data cannot be used to take decisions or other measures against particular individuals, such as full or partial anonymisation, pseudonymisation, and aggregation of data), transparency (especially of the data sources and of the decisional criteria that led to the development of a profile) and data subject's consent and control.

JUST/2014/RRAC/AG/HATE/6652, http://mandola-project.eu/publications, Section 4.2.3.3.2.2 (from which the following steps are extracted).

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 leaflet are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

4.2.5 Data qualities

In the same line of Directive 95/46/EC[166], the GDPR and Directive 2016/680 require that personal data are:

- "*adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed*"[167], the GDPR classifying these principles under the concept of "data minimisation".
- "*accurate and, where necessary, kept up to date*", specifying that "*every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay*"[168], the GDPR classifying these principles under the concept of "*accuracy*".
- "*kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed*"[169], the GDPR naming this principle "storage limitation", and allowing storage for longer periods where data are processed "*solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical*

[166] Article 6 (c, d, e) of Directive 95/46/EC.
[167] Article 5 (c) of the GDPR; Article 4 (c) of Directive 2016/680. For further details see Estelle De Marco and Matthias Eichfeld, *Fundamental principles relating to processing of personal data*, *op. cit.*, Section 3.
[168] Article 5 (d) of the GDPR; Article 4 (d) of Directive 2016/680. For further details see the Estelle De Marco and Matthias Eichfeld, *Fundamental principles relating to processing of personal data*, *op. cit.*, Section 4.
[169] Article 5 (e) of the GDPR; Article 4 (e) of Directive 2016/680.

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 leaflet are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject" [170].

5. Data subject's rights

Both the GDPR and the Directive 2016/680 stipulate specific rights for data subjects to protect the rights and freedoms of natural persons deriving from the Charter of Fundamental Rights of the European Union and the European Convention on Human Rights.

Overview of data subject rights in the GDPR vs Directive 2016/680

Data subject right	GDPR	Directive 2016/680
Right to information	Art. 12-13	Art. 12-14
Right to access	Art. 15	Art. 14-15
Right to rectification	Art. 16	Art. 16
Right to erasure (right to be forgotten)	Art. 17	Art. 16
Right to restriction of processing	Art. 18	Art. 16
Right to data portability	Art. 20	N/A

[170] Article 5 (e) of the GDPR. For further details see the Estelle De Marco and Matthias Eichfeld, *Fundamental principles relating to processing of personal data*, *op. cit.*, Section 5.

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

Right to object to automated individual decision-making	Art. 21-22	N/A

5.1. Data subject's rights in the GDPR

As general modalities to exercise his/her rights, the GDPR states that the data subject must be informed of the action taken pursuant to Articles 15 to 22 in principle without undue delay and in any case within one month (Art. 12, para. 3). In general, all communication between the controller and the data subject shall be in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child (Art. 12, para. 1). In concrete terms, this means that the information should be made available free of charge in written, where appropriate electronic form, in a generally understandable manner for every data subject irrespective of its level of education or expertise. According to Art. 12, para. 7 visualisation in form of standardised icons may be an option to give a meaningful overview.

The Regulation grants the data subject the following rights, which inter alia may be restricted through MS or Union law to explicitly protect the judicial independence and judicial proceedings (Art. 23, para. 1 lit. f):

- **Right of information** (Art. 13 and 14):

  Only if the data subject is adequately informed about the circumstances of the data processing, he/she can exercise his/her rights in an appropriate way. Therefore, when collecting personal

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 leaflet are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

data, the controller is proactively obliged to provide the data subject with information without the requirement of any actions on the side of the data subject. The same obligation applies when the controller intends to further process the personal data for a purpose other than that for which the data were initially collected.

A distinction is made between the personal data the controller collected directly from the data subject (Art. 13) and the personal data that have not been obtained from the data subject (Art. 14). Either way the data subject should be provided with information about

- the identity and the contact details of the controller;
- the contact details of the data protection officer;
- the purposes of the processing as well as the legal basis;
- the recipients or categories of recipients of the personal data;
- in case of an intended data transfer to a third country or international organisation specific information on the level of protection at that location.

According to Art. 13, where the processing is based on Art. 6 para. 1 lit. f, the legitimate interests pursued by the data controller or a third party must also be disclosed.

In case of Art. 14, the data subject must be informed about the categories of personal data concerned.

In addition, the data controller must provide the data subject with further details on the specific circumstances of data processing in

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 leaflet are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission. [96]

accordance with the respective Paragraph 2 of the mentioned articles.[171] Therefore, the data controller should

- specify for which period the personal data will be stored;
- inform about the existence of the rights of the data subject under the GDPR;
- inform about the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal (if processing is based on Art. 6, para. 1 lit. a or Art. 9, para. 2 lit. a);
- inform about the right to lodge a complaint with a supervisory authority;
- inform about the existence of automated decision-making and specify the logic involved, as well as the significance and possible consequences for the data subject.

In addition, in the case of Art. 13, the data subject must be informed as to whether there is a legal or contractual obligation to surrender the data, whether the data are necessary for the conclusion of a contract and what consequences may arise if the data are not made available.

Furthermore, in the case of Art. 14, the data subject should be provided with information about the legitimate interest of the data controller (if processing is based on the legal basis of Art. 6, para. 1 lit. f.) and from which source the personal data originate.

[171] To the purpose of the details to be provided see Article 29 Working party, Guidelines on transparency under Regulation 2016/679, WP260, p. 35-40.

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

→ Regarding the judiciary, the distinction between Art. 13 and Art. 14 is important mainly for the conditions under which the information obligation is not applicable. The data subject that directly handed in a legal document does not have to be informed if he/she already has the respective information (Art. 13, para. 4). Only when personal data have been obtained from another source, the information obligation may furthermore not apply, when obtaining or disclosure of such information is expressly laid down by Union or MS law (Art. 14, para. 5 lit. c). In some MS, it is assumed that the current general procedural rules are sufficient to fill in this opening clause in conformity with Union law. Given that most procedural rules are not intended to protect personal data, there is reason to doubt this solution. Especially since these limitations should be interpreted and applied narrowly.[172]

- **Right of access** (Art. 15):

  In addition to the right to information, the data subject has a right to obtain from the data controller confirmation upon request whether personal data concerning him or her are being processed. Where that is the case, the data subject has a right to be provided with the circumstances and details of the processing pursuant to Art. 15, para. 1 and 2, to allow him/her to determine if the processing is lawful. The information shall be provided by giving a copy of the processed data to the data subject or in a commonly used electronic form, when the

[172] See Article 29 Working party, Guidelines on transparency under Regulation 2016/679, WP260, p. 25.

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

data subject made the request by electronic means (Art. 15, para. 3). The right of access is limited to the extent that it must not affect the rights and freedoms of others (Art. 15, para. 4), which includes possible trade secrets or intellectual property rights according to Recital 63.

→ For the judiciary, this limitation in conjunction with the purpose of general procedural rules can be relevant to deny access for instance in pending proceedings.

- **Right to rectification** (Art. 16):

  Since incorrect data can have negative impact (especially in pending proceedings), the data subject has the right to have inaccurate information rectified without undue delay. Since a similar effect can be caused by incompletely stored data, the data subject shall have the right to complete such data if this is relevant for the purposes of the processing.

  If a correction has taken place without prior request by the data subject, the controller shall inform the data subject of this procedure in accordance with Art. 19.

- **Right to erasure ('right to be forgotten')** (Art. 17):

  A crucial right to maintain control over his/her personal data is the right of deletion in Art. 17 for the data subject. This provision obliges the data controller to delete the respective data without undue delay if one of the following reasons applies:

  - the personal data are no longer necessary in relation to 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 leaflet are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission. [99]

purposes for which they were collected or otherwise processed;
- the data subject withdraws consent on which the processing is based according to Art. 6, para. 1 lit. a, or Art. 9, para. 2 lit. a, and where there is no other legal ground for the processing;
- the data subject objects to the processing pursuant to Art. 21, para. 1 and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21, para. 2;
- the personal data have been unlawfully processed;
- the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;
- the personal data have been collected in relation to the offer of information society services referred to in Article 8, para. 1.

If the respective data was made public by the controller, the so-called 'right to be forgotten' arises from a combination of the obligation to delete and the additional obligation to provide information about this procedure to further data controller (Art. 17, para. 2).

→ With regard to the judiciary, the main reason for deletion is assumed to be that the purpose of the processing has been fulfilled. In this context, old briefs and files need to be examined closely.

However, special attention must be paid to the exemptions in Art. 17, para. 3, where lit. b and lit. d are particularly relevant to 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 leaflet are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission. [100]

Regarding the retention of old judgments, it seems conceivable to justify this with their function as the "memory of the judge", which is indispensable for future decisions and thus serves the performance of a task carried out in the public interest or takes place in the exercise of public authority vested in the controller (lit. b). Nonetheless, such an approach would require a specific legal basis in MS or Union law within the meaning of Art. 6, para. 2 or 3.

In the absence of such legal basis, a classification of the described purposes under archiving purposes of public interest can be considered, which would also lead to an exclusion of the right to erasure (lit. d). In this case, the special requirements of Art. 89 para. 1, in which the principle of data minimisation is also emphasised, must be observed. Therefore, it must be carefully considered whether the files can also be retained without the personal data.

- **Right to restriction of processing** (Art. 18):

  In certain situations, the data subject can request the limitation of processing, namely when

  - it is unclear whether the conditions of an asserted right of the data subject are met, or
  - if a deletion claim exists on the merits, but the data subject has an interest in the data in question not being deleted.

  If such a case is given, the controller shall no longer process, but only store the respective data (Art. 18, para. 2).

- **Right to data portability** (Art. 20):

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

This completely new provision allows data subjects to receive the personal data that they have provided to a data controller, in a structured, commonly used and machine-readable format, and to transmit those data to another data controller without hindrance. Such hindrance could be: fees asked for delivering data, lack of interoperability, excessive delay or complexity to retrieve the full dataset.[173] Necessary condition for the application of this right is that the processing is based on consent or a contract and that it is carried out by automated means. The obvious notion of this right is to prevent vendor lock-in effects. In difference to the right of access the right to data portability aims to offer an easy way for data subjects to manage and reuse personal data themselves[174], which is supported by the possibility to directly transmit data from one controller to another controller, when technically feasible (Art. 20, para. 2).

→ With regard to the judiciary, it should be noted that this right does not apply to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller (Art. 20, para. 3 p. 2).

- **Right to object** (Art. 21):

  As a precondition to exercise the right to object to processing, it is necessary that the processing is based either on legitimate interests of the controller (Art. 6, para. 1 lit. f) or for the performance of a task

[173] See Article 29 Data Protection Working Party, Guidelines on the right to data portability, WP242, adopted on 5 April 2017, p. 15.
[174] See *Ibid.* p. 4.

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

carried out in the public interest or in the exercise of official authority vested in the controller (Art. 6, para. 1 lit. e). In these circumstances, the data subject may at any time object to the processing on grounds relating to his/her particular situation, if there are no overriding compelling legitimate grounds of the data controller (Art. 21, para. 1 p. 2) or the processing is necessary for the establishment, exercise or defence of legal claims. These grounds, which may not be objectively identifiable in the first place, must therefore have a significant impact on the balance of interests. In this way, the data subject is able to correct specific individual cases in which the data controller appears to have lawful, but in fact unlawful data processing due to the particular personal circumstances of the data subject. Complementary, Art. 21 stipulates specific rights to object in case of processing for direct marketing purposes (para. 2) or in case of processing for scientific or historical research purposes or statistical purposes (para. 6).

5.2. Data subject's rights in the Directive 2016/680

Directive 2016/680 also includes a list of data subject rights, including a right of information and a right to access. However, in comparison to the GDPR, the number of data subject rights is less extensive (see table below). In addition, the data subject rights in the Directive can be further restricted. Member States are explicitly granted the opportunity to create restrictions if necessary to avoid obstructing official or legal inquiries, investigations or procedures; avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties;

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 leaflet are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

protect public security; protect national security; or protect the rights and freedoms of others. These restrictions may apply to all data subject rights, i.e., the right to information, the right to access, the right to rectification and the right to erasure.

The right to have personal data erased ('right to be forgotten') and the right to restriction of processing can be found, although in different phrasing than in the GPDR, in Article 16 of the Directive. Instead of erasure, the data controller shall restrict processing where the accuracy of the personal data is contested but cannot be ascertained or when the personal data must be maintained for the purposes of evidence.

The right to data portability (Art. 20 GDPR), i.e., the right for data subjects to receive their personal data in a structured, commonly used and machine-readable format, does not exist in the Directive. This is obvious, as the right to data portability was created to enable data subjects to choose between different providers of products and services, whereas in criminal law the national government has a monopoly on the investigating, prosecuting and sentencing of crimes.

For the judiciary, data subject rights are important as they impose limits to the competences of organizations in the criminal law chain. In case the provisions for processing personal data are not complied with, this may not only affect the rights of a person in the status of a data subject, but also (or more particularly) in the status of a suspect, convict, victim or witness. In regular criminal prosecution processes, the public prosecutors can be corrected by the courts when evidence was illegally obtained (for instance, because a warrant is missing). Such sanctions may be, for instance, excluding

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 leaflet are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

such illegally obtained evidence, lowering the final sentences imposed or concluding that the entire case is not admissible to the court.

5.3. Transparency – comparison between GDPR and Directive 2016/680

GDPR	Directive 2016/680
Transparency is part of the fundamental principles relating to processing of personal data (Art. 5). This is substantiated by the fact that a high degree of transparency is expected from the data controller with regard to information, communication and also the exercise of the rights of the data subject (Art. 12).	It is important to notice that the fundamental principles relating to processing of personal data do not contain transparency (Art. 4) Nevertheless, the Directive requires from the data controller to demonstrate a certain level of transparency with regard to information, communication and also the exercise of the rights of the data subject (Art. 12).
Limitations: • In case of unfounded or excessive requests, the data controller may charge the data subject with a reasonable fee or refuse to act upon the request (Art. 12, para. 5 p. 2); • where the data subject already	Limitations: • In case of unfounded or excessive requests, the data controller may charge the data subject with a reasonable fee or refuse to act upon the request (Art. 12, para. 4 p. 2);

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this leaflet are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission. [105]

has the information (Art. 13, para. 4 / Art. 14, para. 5 lit. a); Further limitations are only permitted where the data were not collected directly from the data subject (Art. 14) and • where the provision of information proves impossible or would involve a disproportionate effort or in so far as the obligation is likely to render impossible or seriously impair the achievement of the objectives of that processing. In such cases the controller should consider appropriate measures including making the information publicly available (Art. 14, para. 5, lit. b); or • where obtaining or	The Directive does not distinguish whether the data were collected directly from the data subject or not with regard to the active information obligation of the controller (Art. 13). But it should be noted, that the Directive refers to "making available" information to the data subject (Art. 13, para. 1). Meanwhile the GDPR refers to "shall provide the data subject with" information (Art. 13, para. 1 of the GDPR), which implies a direct communication with the data subject. In the case of the Directive, the information is to be made publicly available so that every data subject possibly concerned has been the possibility of taking note.[175] This non-transparent approach and the associated restriction of the rights of the data subject can be explained by the fact that, for example, in order to achieve effective criminal

[175] See Article 29 Data Protection Working Party, Opinion on some key issues of the Law Enforcement Directive (EU 2016/680), WP258, adopted on 29 November 2017, p. 17.

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

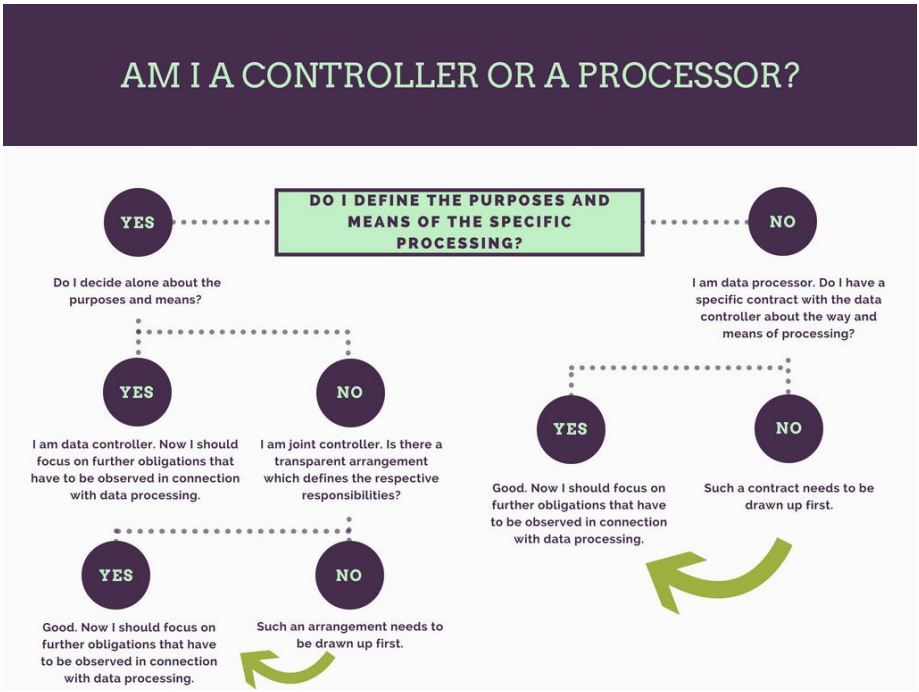
disclosure is expressly laid down by Union or Member State law to which the controller is subject (Art. 14, para. 5 lit. c); or • where the personal data must remain confidential subject to an obligation of professional secrecy (Art. 14, para. 5 lit. d).	prosecution, it is not always possible to make the data subject aware of the processing.[176] However, Art. 13, para. 2 of the Directive provides for the direct supply of specific information to the data subject in special cases. Regardless, according to Art. 13, para. 3 of the Directive the provision of information may be limited where MS adopt appropriate legislative measures in order to • avoid obstructing official or legal inquiries, investigations or procedures; • avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties; • protect public security; • protect national security; • protect the rights and freedoms of others.

[176] *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 leaflet are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

6. Rights and obligations of data controllers & data processors

The following chart helps to determine the respective position in connection with data processing[177]:



[177] The chart does not take into account the different positions within an organisation, therefore every employee should follow the chart "stepping into the shoes" of its employer.

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 leaflet are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

6.1. Data controller & data processor in the GDPR

First of all, the obligations of the data controller because of its central importance as the key person need to be addressed. To improve the overview, a distinction can be made between organisational, technical, institutional and reporting obligations.

The following **organisational obligations** must be taken into account:

- Any processing of data should be preceded by consideration of the risks to the data subject to identify appropriate technical and organisational measures (Art. 24, para. 1), which means a so-called data protection management system (e. g. internal compliance program) needs to be established. In line with the risk-based approach, the data controller should take into account that the data subject may suffer economic or social disadvantages, including discrimination, identity theft or fraud, financial loss, reputational damage or a betrayal of professional secrets. In addition, an increased risk must naturally be considered when processing sensitive data, as well as in the case of processing the data of particularly vulnerable persons, such as minors. The measures identified in this way must be reviewed and updated where necessary. A basic example of such a measure could be the definition of a data protection policy (Art. 24, para. 2).

→ With regard to improper processing in the judiciary, there is a particularly significant risk of social disadvantage for the data subject in the form of future discrimination or reputational damage.

- A crucial innovation of the GDPR is the obligation to provide accountability for all processing activities through a corresponding record

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 leaflet are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission. [109]

(Art. 30), to be able to demonstrate compliance with the data protection regulations of the GDPR (Art. 5, para. 2 / Art. 24, para. 1). With regard to the granularity of such a register, it should be noted that the concept of "processing activity" is not to be equated with the term "processing" as defined in Art. 4 Para. 2, but rather usually comprises a number of processing steps. At this point, a balance must be struck between clarity and attention to detail. In any case, a generation of further personal data by maintaining the register is to be avoided.

- An appropriate degree of data security must be guaranteed (Art. 32). The provision establishes a total of eight criteria 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.

Examples of appropriate measures can be found, for instance, in the catalogue of Art. 29 of Directive 2016/680. In general, pseudonymisation and encryption of personal data should always be contemplated (Art. 32, para. 1 lit. a).

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 leaflet are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission. [110]

Since the first six of the above-mentioned parameters must already be considered in the basic risk evaluation specified in Art. 24, a substantive link is thus created between the prior risk evaluation and data security measures, adding the state of the art and the level of implementation costs as criteria. In view of the current state of the art, the advice of the European Network and Information Security Agency (ENISA) should be consulted. In this context, too, there is an obligation to regularly review the measures (Art. 32, para. 1 lit. d).

→ Regarding the judiciary, the amount of implementation costs as a limiting characteristic appears to be problematic, since in the field of fundamental rights measures may only be rejected due to cost intensity under very strict conditions.

- If the basic risk evaluation comes to the conclusion that a high risk is likely to exist for the rights and freedoms of the data subject, in addition a comprehensive data protection impact assessment (DPIA) must be carried out prior to data processing (Art. 35). Against the background that the DPIA serves to analyse previously unknown processing scenarios and their risks, special focus should be paid to the application of new technologies.[178] However, a single DPIA can cover multiple processing situations that are similar in terms of nature, scope, context, purpose and risks.[179] A DPIA is explicitly indicated if processing is conducted for the purpose of profiling

[178] See Article 29 Data Protection Working Party, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016 /679, WP248rev.01, adopted on 4 April 2017, as last Revised and Adopted on 4 October 2017, p. 7.
[179] *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 leaflet are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

and has legal or similar effects vis-à-vis the data subject. Furthermore, a data protection impact assessment is mandatory if there is extensive processing of sensitive data or data of a highly personal nature or if there is a case of systematic monitoring of publicly accessible areas (Art. 35, para. 3). Regarding the procedure of a DPIA, at least those criteria listed under Art. 35, para. 7 must be taken into account. It seems sensible and logical to follow the steps in the order listed there. In addition, the advice of the data protection officer and, where appropriate, the position of the data subject should be sought (Art. 35, para. 2 and 9).

→ With respect to the processing operations of the judiciary and the question of whether a DPIA is mandatory, the following must be observed: Recital 91 states that when client data is processed by a single lawyer, no DPIA is usually required. In view of the considerably more extensive data processing at the court, it can conversely be assumed that the implementation of a DPIA is necessary.

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 leaflet are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission. [112]

In general, the Art. 29 Data Protection Working Party accordingly proposes the following approach, whereby in practice the individual steps should, if necessary, be carried out several times within on DPIA:[180]

- The data controller is responsible for the selection of data processors, that can guarantee a sufficient degree of data security in the form of suitable technical and organisational measures (Art. 28, para. 1). An appointment of this kind always necessitates a contract that meets the requirements set

[180] The figure is taken from: Article 29 Data Protection Working Party, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016 /679, WP248rev.01, adopted on 4 April 2017, as last Revised and Adopted on 4 October 2017, 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 leaflet are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

out in Art. 28, para. 3.

- Cooperation with the supervisory data protection authority (DPA) in case of a corresponding request should be a basic and self-evident duty (Art. 31).

  → Regarding the judiciary Art. 55, para. 3 must be taken into account, which precludes the judiciary of the ordinary DPA to ensure judicial independence. Instead, it is intended that separate bodies are being created in the judicial system of the Member States, which will be competent for supervising the judicial activities under data protection law. For the activities outside of the judicial capacity, in particular administrative activities, the competence of the ordinary DPA remains unchanged.

Also, **technical obligations** must be considered:

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. Those regulatory approaches pursue in general the implication of the fundamental principles related to data processing and in particular the goal of data minimisation by limiting data collection to the necessary minimum from the outset without further interaction with the data subject.

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 leaflet are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission. [114]

→ With regard to the processing of personal data in the performance of judicial tasks at the moment, the direct scope of this provisions appears to be very limited, at least from a technical point of view, since in many cases those processes do not involve the use of technical products which could be appropriately configured. However, with the increasing application of e-justice instruments, technical limitations will become more and more relevant even for the judiciary in the foreseeable future.

Furthermore, **institutional obligations** must be taken into account:

If the data controller is a public body, or if particularly extensive and regular processing takes place in connection with the surveillance of the data subject, or if sensitive data are processed to a special extent, there is a duty to appoint a data protection officer (Art. 37, para. 1). In such a case, 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/she can actively fulfil his/her obligations to independently advise and monitor the data controller (Art. 39, para. 1). Therefore, involvement of the data protection officer should be included as early as the planning and design stage of data processing (Art. 38, para. 1).

→ It should be noted that judicial activity in courts is explicitly excluded from this obligation (Art. 35, para. 1 lit. a). 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 non-judicial activities, such as the performance of judicial administration tasks.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this leaflet are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission. [115]

Moreover, **reporting obligations** must be considered:

Especially in case of a personal data breach reporting obligations arise. A personal data breach is defined as a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed (Art. 4, sec. 12). In the moment of becoming aware of such a situation, the data controller is subject to reporting obligations to the DPA (Art. 33) and notification obligations to the data subject (Art. 34). These notifications must take place without undue delay, unless there is foreseeably no risk at all to the rights and freedoms of the data subject (Art. 33, para. 1) or the breach is unlikely to result in a high risk for the respective rights of the data subject (Art. 34, para. 1 and 3). In addition, a notification of the data subject is not necessary if one of the exemptions stipulated in Art. 34, para. 3 applies.

In general, it is therefore necessary to conduct a specific risk assessment which, according to recitals 75 and 76, must focus primarily on the likelihood and severity of the risks for the data subject. According to Art. 29 Data Protection Working Party the assessment should in detail include the type of breach, the nature, sensitivity and volume of personal data, ease of identification of individuals, the severity of consequences for individuals, the number of affected individuals, special characteristics of the individual and of the data controller.[181]

[181] Article 29 Data Protection Working Party, Guidelines on Personal data breach notification under Regulation 2016 /679, WP250rev.01, adopted on 3 October 2017, as last Revised and Adopted on 6 February 2018, 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 leaflet are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

→ According to Art. 23, para. 1 lit. f, the notification obligation vis-à-vis the data subject (Art. 34) may be restricted by Member States' regulations in order to preserve the independence of the judiciary and to protect legal proceedings. Moreover, it should be noted in this context that the notification must be made to the competent DPA. 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, must be informed.

—

In comparison to the data controller, the **obligations of the data processor** are very similar but differ in some manners due to the fact that the processor is subject to instructions of the controller (Art. 28, para. 3). Since the data controller is only permitted to cooperate with a data processor that complies with Art. 24 and 25 (which are solely addressed to the controller), an indirect obligation regarding these provisions is implied on the processor (Art. 28, para. 1). On the other hand, data processors are directly obliged to maintain a register of their processing activities (Art. 30, para. 2) and directly responsible for ensuring adequate data security in accordance with Art. 32, para. 1.

The inclusion of further data processors is only allowed with the appropriate permission of the respective data controller (Art. 28, para. 2). Even after approval has been granted, the first contract data processor is still liable to the data controller for any misconduct of the second data processor (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 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 leaflet are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission. [117]

Though the GDPR intends a close connection between controller and processor, it is important to emphasize that the processor has an independent responsibility for compliance with the respective GDPR regulations which is reflected in the possibilities of liability and sanctions (Art. 82 and 83).

6.2. Data controller & data processor in the Directive 2016/680

For data controllers, a list of obligations with regard to the processing of personal data is included in both Directive 2016/680 and the GDPR. The table located under 6.3 provides an overview. These data controller obligations are to a large extent similar and address data protection by design and by default, maintaining records of the data processing activities, logging, mandatory cooperation with the Data Protection Authorities (DPAs), performing data protection impact assessments, ensuring security of the processing of personal data, mandatory notifications to supervisory authorities and/or data subjects in case of data breaches, prior consultation with the DPA in case of high risks and designating data protection officers.

For logging of processing operations there exists a special provision on Article 25 of the Directive. The implementation of logs is a crucial tool for data protection monitoring, hence for controlling all relevant data processing operations. In order to do so, it should be possible to trace user activity to spot abusive use. National laws should further develop the requirements for logging: on content, on storage periods, on technical measures, on self-auditing and on internal policies to promote compliance.[182] Data protection

[182] WP29 (2017) Opinion WP 2017/258 on some key issues of the Law Enforcement Directive (EU 2016/680). Adopted 20 November 2017.

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

officers must be involved in the definition of the procedure in order to effectively delete or erase the data once the time limits for the storage have expired.[183] All competent authorities should designate a data protection officer (DPO) according to article 32.

Member states can opt to exempt courts and other independent judicial authorities from the obligation to designate a data protection officer for processing operations when they act in their judicial capacity. The GDPR encourages the use of codes of conduct (Art. 40-41 GDPR) and certification (Art. 42-43 GDPR), but the Directive does not contain similar provisions.

It is important to note that the data controller obligations also apply to data processors. Data controllers and data processors are not always the same entities. When data processors violate provisions in the directive, they can be held accountable for this, but the data controller can also be held accountable.

→ For instance, when a court outsources the structuring and analysis of its court files to a technological company, the court remains the data controller, but the technological company is a data processor. When the technological company is confronted with a data breach, the court is responsible and liable. Whether the technological company is also responsible and liable depends on the nature of the data breach and the exact circumstances.

6.3. Comparative table for GDPR and Directive 2016/680

Data controller obligation	**GDPR**	**Directive 2016/680**

[183] WP29 (2017) Opinion WP 2017/258 on some key issues of the Law Enforcement Directive (EU 2016/680). Adopted 20 November 2017.

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

Data protection management system	Art. 24	Art. 19
Data protection by design	Art. 25, para. 1	Art. 20, para. 1
Data protection by default	Art. 25, para. 2	Art. 20, para. 2
Maintain records	Art. 30	Art. 24
Logging	N/A	Art. 25
Cooperation with the DPA	Art. 31	Art. 26
Data protection impact assessment	Art. 35	Art. 27
Security of processing	Art. 32	Art. 29
Data breach notification	Art. 33-34	Art. 30-31
Prior consultation with the DPA	Art. 36	Art. 28
Data protection officers	Art. 37-39	Art. 32-34

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 leaflet are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission. [120]

7. Transfer of personal data to third countries

The transfer of personal data to third countries and international organizations is regulated in Chapter V of the GDPR. Judiciary should be extra careful when requesting documents or actions from third countries/organisations or when granting requests of third countries/organisations to provide documents or actions. Requests and documents that judiciary sent contain personal data of the parties to the case (such as names, addresses, etc.) and/or information of criminal offences.

The motivation behind the restrictions of such transfers is that some countries outside the EU may not provide data protection, comparable with the one provided in Member States. This could be used by some entities to circumvent the requirements of the GDPR. That is why transfers to third countries are permitted in four cases (regarding judiciary):

1. When there is an adequacy decision. The adequacy decision is an act taken by the European Commission and it is based on an assessment whether the third country (or separate sectors/territories from a country) or the international organization ensures an adequate level of protection. According to the CJEU1, even though the means a third country uses to ensure such a level of protection may differ from those in the EU, they must prove effective in practice, in order to ensure protection equivalent to that guaranteed within the EU. According to the WP29's recommendations, the third country must include in its framework specific provisions that address concrete aspects of the right to data protection. Once there is such an adequacy decision, the transfer does not require any specific authorisation. When requesting documents/actions

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 leaflet are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

and when granting request for documents/actions judiciary should pay attention to the acts of the European Commission and be aware which countries' legislation is rendered compliant with the requirements. The Commission publishes in the Official Journal of the European Union and on its website a list of the third countries and international organisations for which it has decided that an adequate level of protection is ensured.

2. When there is an international agreement which includes appropriate safeguards for the data subjects. Recital 102 of the GDPR stipulates that the Regulation does not affect the existing international treaties. Many countries have signed mutual legal assistance treaties and based on them judiciary may provide or request certain information, documents or actions. It is important for judiciary that such interaction would almost certainly result in data transfer.

   According to Art. 48, any judgment of a court or tribunal and any decision of an administrative authority of a third country requiring transfer of personal data may only be recognised or enforceable if it is based on an international agreement.

3. In the absence of an adequacy decision and an international agreement, personal data may be transferred to a third country only if appropriate safeguards are provided by the sender, and if enforceable data subject rights and effective legal remedies for data subjects are available. Such safeguards relevant to judiciary may be legally binding and enforceable instruments or provisions in administrative arrangements between public authorities or bodies.

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 leaflet are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission. [122]

4. Specific situations – the GDPR permits transfers even if one of the already mentioned cases is not present. The most relevant to judiciary exceptions in special situations are: a) when the transfer is necessary for important reasons of public interest, and b) when the transfer is necessary for the establishment, exercise or defence of legal claims. The use of these exceptions must be justified by the judiciary.

There is low probability that judiciary will have to apply these provisions often, as most of the time data will be transferred on the basis of bilateral agreement with the third country or on the basis of adequacy decision.

As some structures within the judiciary perform tasks under Art. 1 of Directive 680/2016, judiciary should bear in mind that in some cases the provisions of the Directive may be applicable to transfers to third countries instead of those of the GDPR. The rules in this regard are established in Chapter V, Articles 35-40 of the Directive. The following key differences between the Directive and the Regulation could be extracted:
1) the Directive establishes additional conditions that should be fulfilled cumulatively when transferring data to third countries and international organizations. They are:

- the transfer should be necessary for the purposes of Article 1(1) of the Directive;
- the receiver in the third country should be an authority competent for the purposes in Article 1(1);
- where personal data are transmitted or made available from another Member State, that Member State should have given a prior authorisation to the transfer in accordance with its national law;

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 leaflet are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission. [123]

- there should be an adequacy decision of the Commission, appropriate safeguards or one of the derogations for specific situations should apply;
- All onward transfers should be authorised by the country of the original transfer after taking into account all relevant factors (except in cases of immediate and serious threat to public security or to essential interests of a Member State).

2) under the Directive the enlisted appropriate safeguards, which could be applied in the absence of an adequacy decision, are only two: safeguards in a legally binding instrument and full assessment of all the circumstances surrounding the transfer of personal data made by the sender. Such legally binding instrument, according to Recital 71, may be a bilateral agreement or a cooperation agreement with organisations like Europol and Eurojust.

3) the cases in which the authorities could transfer data in the absence of appropriate safeguards and an adequacy decision are different under the Directive:

- in order to protect the vital interests of the data subject or another person;
- to safeguard legitimate interests of the data subject, where the law of the Member State transferring the personal data so provides;
- for the prevention of an immediate and serious threat to public security of a Member State or a third country; this base for transfer is much narrower that the public interest listed in the GDPR.
- in individual cases for the purposes of Article 1(1);
- in an individual case for the establishment, exercise or defence of legal

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 leaflet are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission. [124]

claims; in the GDPR the legal claims are also a legitimate ground to execute the transfer, but in the Directive the claim should be explicitly connected with the purposes of Article 1(1).

4) Regarding international agreements, Art. 61 of the Directive stipulates that the agreements in the field of judicial cooperation in criminal matters and police cooperation which are concluded before 6 May 2016 and which comply with Union law stay in force. In contrast to the GDPR, in the Directive there is no explicit provision regarding future agreements in this field.

5) Additionally, Art. 39 of the Directive provides for another exception. It concerns the requirement the recipient to be an authority competent for the purposes in Article 1(1). Art. 39 permits the transfer to recipients in third countries which are not a competent authority under the Directive in individual and specific cases, when all the other requirements of the Directive are fulfilled, and all of the following conditions are observed:

- the transfer is strictly necessary for the performance of a task of the sender for the purposes in Article 1(1);
- the sender made an assessment that no fundamental rights and freedoms of the data subject override the public interest from the transfer;
- the sender considers that the transfer to an authority that is competent for the purposes in Art. 1(1) in the third country is ineffective or inappropriate, in particular because the transfer cannot be achieved in good time;
- the authority that is competent for the purposes in Art.1(1) in the third country is informed without undue delay, unless this is

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 leaflet are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission. [125]

ineffective or inappropriate;

- the sender informs the recipient of the specified purpose or purposes for which the personal data are only to be processed, provided that such processing is necessary.

Judiciary should also bear in mind that the adequacy decisions, adopted under the old Directive 95/46/EC, are not valid under Directive 680/2016, as opposed to under the GDPR.

Judiciary should be extra careful when transferring data to third countries as part of activities that may be in the scope of the Directive, as it introduces different conditions that must be fulfilled cumulatively.

8. Legal remedies available to data subjects

8.1. Right to lodge a complaint with a supervisory authority

When the data subject considers that the processing of personal data relating to him or her may be infringing upon the Regulation, the data subject has the right to lodge a complaint with a supervisory authority. This right is without prejudice to any other administrative or judicial remedy that may be available to the data subject.

The supervisory authority with which the complaint is lodged will likely be the supervisory authority in the Member State of the habitual residence of the data subject, or the place of work of the data subject, or of the place of alleged infringement (Art. 77, para. 1 of the GDPR; Art. 52, para. 1 of the Directive).

However, it should be stressed that according to Article 55, para 3 of the GDPR and Article 45, para 2 of the Directive, the supervisory authorities

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 leaflet are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

shall not be competent to supervise processing operations of courts acting in their judicial capacity. For processing that is performed in another capacity (as an employer for instance) the supervisory authority shall be competent.

The supervisory authority must inform the complainant of the progress and outcome of the complaint. If the supervisory authority deems that competence over the complaint falls within another supervisory authority, it must transmit the complaint to the latter without undue delay. The supervisory authority must also provide further assistance upon request by the data subject (Art. 77, para. 2 of the GDPR; Art. 52, para. 2-4 of the Directive).

The data subject has the right to be informed by the controller about his or her right to lodge a complaint with a supervisory authority, as well as to receive all necessary information in that regard (e.g. contact details of the controller or its representative):

- when personal data are collected from the data subject (Art. 13, para. 2 lit. d of the GDPR)
- when personal data have not been obtained from the data subject (Art 14, para. 2 lit. e of the GDPR)
- when the controller does not take action on a request by the data subject (Art. 12, para. 3 of both GDPR and Directive)

The same provisions apply in cases of infringement of data subject's rights under the 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 leaflet are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission. [127]

→ Courts do not have the power to decide on their own on the lawfulness of the way the supervisory authority deals with a complaint lodge by a data subject. However, they obtain such power when a data subject comes to justice against the supervisory authority alleging failure to adequately deal with his or her complaint. This case is covered by the right to an effective judicial remedy against a supervisory authority, contained in Art. 78 of the Regulation and Art. 53 of the Directive.

The possible infringement of this right of the data subject may be the failure to inform the subject about his right to lodge a complaint with a supervisory authority. In such a case, the judiciary shall evaluate whether the existence of such right was adequately made known to the subject by the controller or processor. This must have been done actively and the relevant contact information for making such a complaint (namely example telephone number, address and e-mail address of the relevant supervisory authority) must have been provided.

8.2. Right to an effective judicial remedy against a supervisory authority

The data subject has the right to an effective judicial remedy against a Supervisory Authority:

- in the case of a legally binding decision affecting them
- in the cases where the supervisory authority did not handle a complaint or did not timely inform the complainant about the progress and outcome of their complaint.

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 leaflet are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission. [128]

Such judicial remedy may be sought in the competent courts of the Member State of the supervisory authority.

The exercise of such judicial remedy does not prejudice the availability to the data subject of any other administrative or non-judicial remedy (Art. 78 of the GDPR; Art. 53 of the Directive).

The supervisory authority must forward to the court any decision or opinion of the European Data Protection Board that precedes the decision of the supervisory authority which is challenged in court (Art. 78, para. 4 of the GDPR).

The provisions are identical in the Directive as well, except paragraph 4 of the GDPR which oblige the supervisory authority to forward to the court, a potential opinion or decision of the Board.

→ A likely possible infringement case could be a legally binding decision of the authority affecting the data subject. For example, a failure of the supervisory authority to recognize the infringement and wrongfully dismissing the complaint. In this case, the judiciary shall check the merits of the supervisory authority's decision and may be called to alter such decision in favour of the data subject.

Another infringement case could be the failure of the supervisory authority to adequately address such a complaint. For example, when the supervisory authority does not handle or investigate the complaint within a reasonable period (Art. 57, para. 1 lit. f of the GDPR), indirectly allowing the continuance of the infringement. In addition, the case where the supervisory authority does not timely inform the complainant about the progress and outcome of their complaint (Again relevant provision is Art. 57 para. 1 lit. f 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 leaflet are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission. [129]

A claim may possibly be made not only by a natural person, but also by a legal person who believes that a condemnatory decision of a supervisory authority against it is wrong.

It could be good practice that the courts get familiar with the obligations of the supervisory authority not only as provided for in the Regulation (which is a generic guideline) but specifically with the directions given by the governmental institution in each Member State with which the supervisory authority ought to comply.

8.3. Right to an effective judicial remedy against a data controller or processor

In cases where the data subject decides to take judicial measures for an infringement with his rights regarding his personal data, he must enjoy an effective judicial remedy.

When the data subject considers that the processing personal data relating to him or her may be infringing upon the Regulation, the data subject has the right to effective judicial remedy against a controller or processor. This right is without prejudice to any administrative or non-judicial remedy that may be available to the data subject.

Such legal action may be brought:

- before the courts of the Member State where the controller or processor has an establishment (in cases falling under the scope of the Regulation but where controller or processor do not have an

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 leaflet are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

establishment in a Member State, the establishment of the representative designated under Art. 27 of the GDPR); or

- before the courts of the Member State of habitual residence of the data subject. This alternative jurisdictional basis is not available when the controller or processor is a public authority of a Member State acting in the exercise of its public powers (Art. 79 of the GDPR; Art. 54 of the Directive).

The data subject has the right to be informed by the controller about his or her right to seek effective judicial remedy, when the controller does not take action on a request by the data subject (Art. 12, para. 3 of both GDPR and Directive).

The provision is the same in the Directive, except that the Regulation moves a step forward and provide guidance regarding the forum for such claim.

→ It is important for the judiciary to have a clear picture of who may be the controller and the processor (these are usually the entity collecting and processing the personal data, i.e. a company) as well as the rights and obligations of the controller and the processor against the data subjects. These are explained in Regulation Chapter IV and in Directive Chapter IV.

Because the controller and the processor are ultimately responsible for the personal data to be legally collected and processed without threatening the rights of the data subjects, the scenarios under which they may be held liable are various. For example, when the data are processed without the subject's consent (Art. 6, para. 1 lit. a of the GDPR) when the subject is not informed

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 leaflet are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission. [131]

about or is denied of his rights regarding the process of his or her data [Reg. Chapter III, Dir. Chapter III] and when the subject is not made aware of a potential breach of his data, given that this is possible to lead to high risk for his or her rights and freedoms (Art. 34, para. 1 of the GDPR, Art. 31, para. 1 of the Directive).

8.4. Right to compensation and liability

Data subjects have the right to full and effective compensation against the controller and the processor, for material or non-material damage suffered as a result of infringement of the Regulation (Art. 82, Rec. 146 of the GDPR).

Such legal action may be brought:

- before the courts of the Member State where the controller or processor has an establishment (in cases falling under the scope of the Regulation but where controller or processor do not have an establishment in a Member State, the establishment of the representative designated under Art. 27 of the GDPR); or

- before the courts of the Member State of habitual residence of the data subject. This alternative jurisdictional basis is not available when the controller or processor is a public authority of a Member State acting in the exercise of its public powers (Art. 82 and 79, Rec. 147 of the GDPR; Art. 56 of the Directive).

Liability for any damage caused by processing which constitutes an infringement of pertinent rules rests principally with the controller, if involved in the processing that led to the damage.

The processor is liable when:

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 leaflet are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

- it has not complied with the obligations specifically addressed to processors under Regulation or Directive / implementing legislation; or

- it has acted outside of, or contrary to, lawful instructions of the controller.

Each of the controllers and/or processors who are involved in the same processing and are responsible as described above, is liable for the entire damage suffered and may upon payment of full compensation claim back from the other controllers and/or processors the part of the compensation corresponding to their part of the damage (joint and severable liability).

A controller or processor is exempt from liability if it proves that it is in no way responsible for the event giving rise to the damage.

The same right exists for infringement with Directive or national provisions implementing the Directive (Art. 56, Rec. 88 of the Directive). However, the provisions under the Regulation are much more extensive rather than the more general and simple provision founded in the Directive.

Under the Directive, the data subject may also seek compensation from any authority competent under Member State law, under Art. 56 Dir.

→ Judges will inevitably come across difficult cases, where it is strongly contested whether the infringement did result in damage to the data subject, and what kind damage. Inevitably, the measure of compensation may differ depending on the nature of the damage, i.e. material or non-material. This does not belie the fundamental principle that, once it has been established that damage took place due to the processing by the controller or processor, these actors will be liable.

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 leaflet are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission. [133]

In cases where infringement is alleged and compensation claimed, the judge shall investigate the relevant authorisation given by the data subject, if such has been given and whether it relates to the specific type of processing which resulted to the infringement. Detailed investigation of the facts of the case is thus required.

An important consideration is involving the appropriate forum for each action. Such cases can be brought only before the courts of the Member State of the controller or processor's establishment, and where these do not have an establishment in a Member State, then the courts of the establishment of their representative. Alternatively, a case can be brought before the courts of the Member State of habitual residence of the data subject. The only exception relates to cases where the controller or processor is a public authority of a Member State acting in the exercise of its public powers, making it unable to bring a case before the courts of the Member State of habitual residence of the data subject.

It should also be kept in mind that the responsibility is joint and severable on the controller and processor. However, it must be underlined that the processor is only co-liable in certain cases exhaustively provided for in the GDPR (Art. 82, para. 2).

There is the presumption that the controller and processor are liable. The burden of proof is reversed and lies on the controller and processor to proof that they are in no way responsible for the event giving rise to the damage, leading to a standard of proof admittedly high.

As it relates to the Directive, the same right for compensation and liability is also available against any authority competent under Member State law.

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 leaflet are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission. [134]

8.5. Right to be represented

The data subject has the right to mandate a not-for-profit body, organisation or association active in the field of protecting of data subjects' rights and freedoms as to their personal data to take one or more of the following actions on his or her behalf:

- lodge a complaint against a controller or processor with the supervisory authority

- seek effective judicial remedy against a controller or processor

- seek compensation from the controller or processor for the material or non-material damage suffered

- seek effective judicial remedy against a supervisory authority.

Such entity must be duly constituted and have public-interest statutory objectives.

Additionally, national law may allow such entities to lodge such a complaint or seek such judicial remedy (apart from compensation) independent of the data subject affected (Art. 80 of the GDPR; Art. 55 of the Directive).

The right is provided for in both the legal instruments as well as the requirements which the mandated body shall fulfil.

However, the Regulation additionally allows such a body to commence such legal procedures for the data subject without being mandated for doing so by the data subject, if it is of the opinion that his or her rights under the Regulation have been infringed as a result of the processing.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this leaflet are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission. [135]

In addition, the right of data subjects to representation should be without prejudice to Member State procedural law, which may require mandatory representation of data subjects in court by a lawyer (Rec 87 of the Directive).

→ A court action is important to be filed by the correct claimant and against the correct defendant, which determines eventually the life of a potential court action.

The person/entity which begins the procedures either of a complaint with a supervisory authority, seeking judicial remedy against a controller or a processor or a supervisory authority as well as the legal procedure of seeking compensation, can be not only the data subject but also a non-for-profit body, organisation or association which fulfils certain requirements set by the Regulation (Art.80, para. 1 of the GDPR; Art.55, para. 1 of the Directive).

However, it must be underlined that this right does not infringe the civil procedure rules of a Member State which may require the representation in court by a lawyer.

As for the cause of action, it is important to note that the Regulation allows the non-for-profit body to commence such procedure even when not mandated by the data subject, if of the opinion that the rights of a data subject under this Regulation have been infringed as a result of the processing.

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this leaflet are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission. [136]

INTRODUCTION OF THE DATA PROTECTION REFORM TO THE JUDICIAL SYSTEM
INFORM

Appendix: Helpful literature

- INFORM Deliverable 2.1 – Review report on the GDPR for the judiciary
- INFORM Deliverable 2.2 – Review report on the Directive 2016/680 for the judiciary
- INFORM Deliverable 2.4 – Review report on the GDPR for legal practitioners
- INFORM Deliverable 2.5 – Review report on the Directive 2016/680 for legal practitioners
- INFORM Deliverable 2.7 – Review report on the GDPR for court staff
- INFORM Deliverable 2.10 – Comparative analysis on the differences between Directive 95/46/EC and GDPR
- INFORM Deliverable 2.11 – Data Protection Glossary
- Rücker/Kugler – New European General Data Protection Regulation – A Practitioner's Guide, *C.H.Beck/Hart/Nomos* – 2017
- Voigt/von dem Bussche – The EU General Data Protection Regulation (GDPR) – A Practical Guide, *Springer* – 2017

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this leaflet are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission. [137]