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 court staff

Contributing partners: eLAW, 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.

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: MU Contributions from: eLAW, ITTIG, LIF, UCY, UGOE, UNIBA	May 2nd 2018
Version 2	Updated by contribution from LIF	May 15th 2018
Version 3	Updated by contribution from UGOE	May 17th 2018
Version 4	Reviewed and updated by MU	May 18th 2018
Version 5	Updated by contribution from UCY, edited by MU	May 21st 2018
Version 6	Reviewed by LIF	May 29th 2018
Version 7	Reviewed by UNIBA	June

This project is funded by the 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.

		11th 2018
Version 8	Updated by contribution from ITTIG, edited by MU based on reviews	June 11th 2018
Version 9	Updated by UGOE based on reviews	June 13th 2018
Version 10	Updated by ITTIG based on reviews	June 14th 2018
Version 11	Updated by eLAW based on reviews	June 20th 2018
Version 12	Final editing by MU	June 21st 2018
Version 13	Reviewed by LIF	July 18th 2018
Version 14	Updated by MU	July 26th 2018
Version 15	Reviewed by LIF	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.

Executive summary

As of 25th May 2018 the European data protection reform package with General Data Protection Regulation (GDPR) and the 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 GDPR and the Directive 2016/680 by the target groups, which are the judiciary, legal practitioners, and the court staff.

The following guidelines provide a summary of applicable provisions of GDPR and the Directive 2016/680 for the specific activities of the court staff category. The content is based on in-depth review and other INFORM project documents that provide further details on specific issues.

This project is funded by the 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.

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.

This project is funded by the 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.

Contributing Partners

eLAW – Chapter 2, summary tables in Chapters 5 and 6

ITTIG – Chapter 3

LIF – Chapter 7

MU – Chapters 1, 4, 6, 8.1, 8.2 and 8.4

UCY – Chapter 8.3

UGOE – Chapter 5

Reviewing Partners

MU

LIF

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.

List of Abbreviations

CEPEJ	European Commission for the Efficiency of Justice
CJEU	Court of Justice of the European Union
DDoS	Distributed denial of service
DPA	Data protection authority
DPO	Data protection officer
ECHR	European Court of Human Rights
ENISA	European Union Agency for Network and Information Security
EU	European Union
Eur. Court of HR	European Court of Human Rights
GDPR	General Data Protection Regulation (EU) 2016/679
HR	Human resources
ICT	Information and communication technology
IP	Internet protocol
IT	Information technology
MS	Member State
SJC	Supreme Judicial Council
WP	Working Party

This project is funded by the 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 to the guidelines

1.1. Objective of the guidelines

These guidelines are aimed to provide summary description of applicable provisions of GDPR and Directive 2016/680 for the specific activities of the court staff category. The content is based on in-depth review and other INFORM project documents that provide further details on specific issues.

1.2. Definition and scope of the court staff category

The general EU-wide approach to definition of the court staff category presents specific challenges because the framework organisation of court system is different in each Member State.[1] Court staff represents a body of court personnel, who alongside judges provide a crucial component of the functioning judicial system. The composition of the core court staff has to understandably differ between various judicial branches and instances, as the necessary administrative positions vary in consequence of the particular operations of the court.

Of particular importance are all operations that directly come into contact with the court files, evidence or other documents or information essential for the court proceeding. These are particularly performed by the "Rechtspfleger", meaning the high-ranking judicial officials to whom judicial tasks have been transferred, who therefore work independently alongside judges and have capacity to issue judicial decisions in certain categories of cases. Equally relevant are the operations of the registry office of the court;

[1] Roberta Ribeiro Oertel and Peter IB Goldschmidt, 'The Training of Court Staff and Bailiffs at the European Union Level' in Directorate-General for Internal Policies of Union (ed), *The Training of Judges and Legal Practitioners* (European Parliament 2017) <http://www.europarl.europa.eu/RegData/etudes/IDAN/2017/583134/IPOL_IDA(2017)583134_EN.pdf> accessed 19 April 2018. p. 41.

This project is funded by the 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.

clerks and registrars, who provide various supporting functions to the judge during the proceeding including the record keeping; the registry of the court files; the security office of the court; and the evidence and record keeping department.

Additional to the aforementioned court staff directly assisting the judge or handling the court files, there are numerous functions and roles that provide indirect support to the court operations. Most importantly, the predominant number of courts includes an IT-department with administrators of court information systems, networks, databases and applications. The management of a court is usually performed by the president of the court, who is supported by secretariat or president's office as well as standard departments like the human resources, public relations or economic departments. Some higher courts also have an analytical department that analyses the available case law and organizes the training and education of judges and judge assistants. Alternatively some of these functions can be performed by the court library or other country-specific structures and departments.

Various Member States further report particular functions that fall within their perception of court staff that are not similarly reflected in other Member States. To better illustrate the variety, several examples follow: judicial trainees, people in charge of serving court documents (on the parties), press centre and telephone exchange (Czech Republic); court interpreters (Estonia); assistants, receptionists, porters (Italy); translators (Lithuania); assistance magistrates, judicial assistants, probation counsellors

This project is funded by the 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.

(Romania).[2] There are also functions of staff at the courts of Member States that are bordering the scope of court staff definition, e.g. the judicial guard (marshals), who process personal information *inter alia* through the record of visitors to the court. In multiple Member States the court structure also includes assistant or trainee judges, who are, however, closer to the judiciary category.

Similarly as the court staff fulfils supporting roles for the judiciary, the staff attached to the public prosecutors assists with various tasks that may include work on files like case research or preparation of evidence, or auxiliary functions necessary for day-to-day operations of the office including administration, secretariat or IT support.

1.3. Structure and administration of judiciary

The broad scope and high variety in specific definition of court staff among Member States reflects the different national judicial traditions and contrasts between structural models of judiciary in general. These differences need to be taken into consideration, as they may have direct impact on specific obligations and requirements under GDPR and Directive 2016/680. Some Member States established a judicial council (e.g. Bulgaria, Estonia, or Hungary), other have numerous administrative tasks performed by central administrative agency (e.g. board of governors in Denmark, *Oficina Judicial* in Spain) or department of the Ministry of Justice (e.g. Czech Republic,

[2] CEPEJ, 'Study on the Functioning of Judicial Systems in the EU Member States. Facts and Figures from the CEPEJ 2012 -2014 Evaluation Exercise' <http://ec.europa.eu/justice/effective-justice/files/cepj_study_scoreboard_2014_en.pdf>. pp. 256-258.

This project is funded by the 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.

Germany, or Italy).[3] There may also be courts with specific regime, e.g. military courts or maritime courts.

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

GDPR and Directive 2016/680 represent the core of data protection law reform. The basic concepts are based on the Data Protection Directive 46/95/EC, Council Framework Decision 2008/977/JHA respectively and develop upon the personal data protection tradition established through the directive in the Member States.

The variety of approaches to the institutional organisation of judicial bodies in the Member States necessitates open formulations in the European level legislation that should be further specified in national law. Due to the role of judiciary as public system of dispute resolution and pursuit of justice, many fundamental principles of personal data protection and obligations required by GDPR and Directive 2016/680 are inherent to the existing operational and functional framework of the judicial system.

This section deals with the scope of application of these legal instruments. Section 2.1 explains the subject matter and objectives, the material and territorial scope of the GDPR. Section 2.2 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. data processing within the prevention, investigation, detection or

[3] For more details refer to The European e-Justice Portal. 'Judicial systems in Member States' <https://e-justice.europa.eu/content_judicial_systems_in_member_states-16-es-en.do?member=1> accessed 19 April 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.

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.

2.1. GDPR scope

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 movement of personal data (Article 1, para. 1 GDPR). 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 (Article 1, para. 2 GDPR) and, on the other hand, it aims to ensure free movement of personal data within the EU (Article 1, para. 3 GDPR).

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 (Article 2, para. 1 GDPR).

Material scope of the GDPR focuses on the processing of personal data. The concept of personal data (defined in Article 4, para. 1 of the GDPR) 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 (Article 4, para. 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.

This project is funded by the 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.

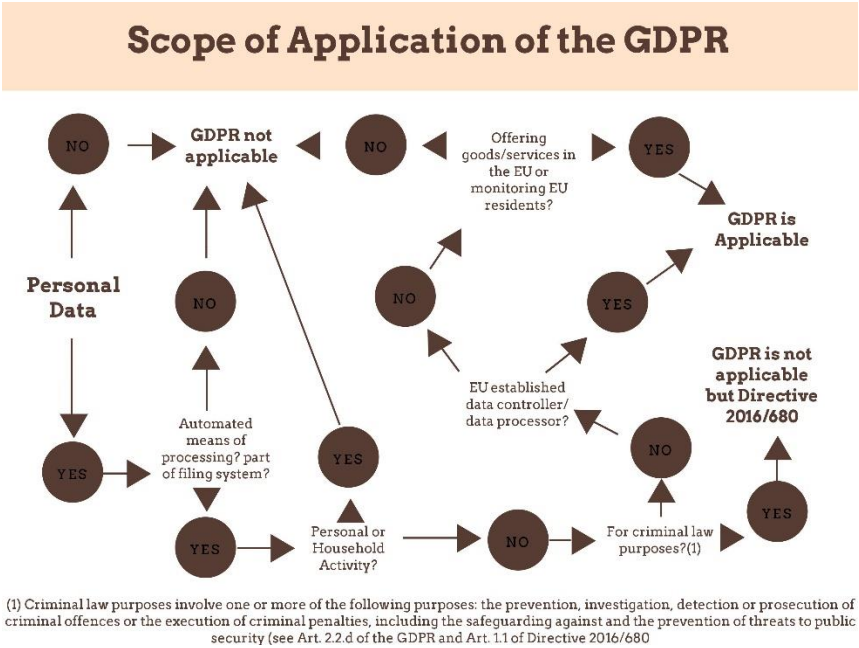
Some forms of processing of personal data are excluded from the scope of the GDPR. For instance, the processing of personal data by a natural person in the course of a purely personal or household activity is beyond the scope of the GDPR (Article. 2, para. 2 lit. c GDPR).

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, 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 Article 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 of the GDPR). 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.



2.2. Directive scope

The 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 Article 2, para.2 lit. d of the GDPR). The **subject matter and objectives** of the Directive are described in Article 1 of the Directive 2016/680. The Directive lays down the rules relating to the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal

This project is funded by the 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.

penalties, including the safeguarding against and the prevention of threats to public security (Article 1 of the Directive). 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 (Article 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 (Article 1, para. 2 lit. b of the Directive).

The Directive focuses on data processing by so-called competent authorities, which is defined in Article 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 (Article 1 and 2 of the Directive). This includes the safeguarding against and the prevention of threats to public security (see also Recital 11 of the Directive). As such, it should be noted that not all personal data processed by law enforcement agencies and the judiciary (when processing criminal law cases) is within the scope of the Directive. For instance, when law enforcement agencies or the judiciary are 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.

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 for the purposes set in Directive 2016/680 by these organizations, this processing will be within the scope of the Directive. The scope of the Directive covers only the prevention, investigation, detection or prosecution of criminal offences and the execution of criminal penalties.

Also, when others than the competent authorities collect and process personal data on criminal cases, the processing of these data is 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 national authorities in specific cases and in accordance with national law (see Recital 11 of the Directive). These financial institutions are not considered

This project is funded by the 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.

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 of the Directive).

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 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-

[4] See also Recital 26 of the Directive.

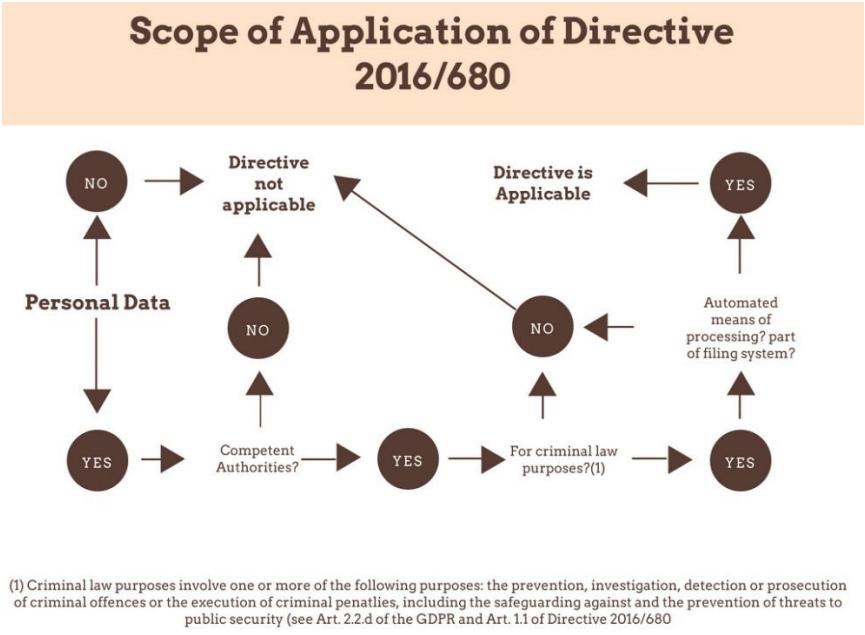
[5] Note that preparing serious crimes is a punishable offence (and hence a crime in itself) in most jurisdictions.

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.

digitalized data that 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 by EU institutions, bodies, offices and agencies (Article 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 members of courts staff 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 GDPR and the Directive 2016/680, in order to be compliant with them. The aim of this chapter of the Guidelines is to contribute to an in-depth and accurate knowledge of the meaning of the issues (pseudonymisation, types of data, data processing) surrounding the concept of "personal data" under the GDPR and 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 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.

This project is funded by the 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

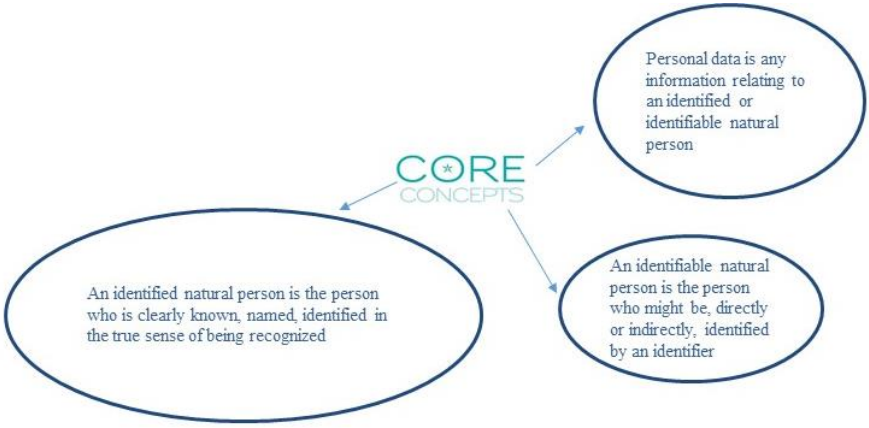
The homogeneity of the definitions of "personal data" provided by the Directive (Article 3 para. 1) and by the GDPR (Article 4 para. 1) contributes to harmonize level of data protection between Member States. Court staff would benefit of this consistency when processing personal data in their daily activities.

Directive 2016/680	***GDPR***
Art. 3 para. 1	Art. 4 para. 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 reflect the intention of the European legislator for 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.

Core concepts



In particular

Data that falls outside the application of GDPR is:

- data of deceased persons
- 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

This project is funded by the 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 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, etc. which might be indirectly identifies a person
- a location or address
- 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

This project is funded by the 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.

"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).*

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).

This project is funded by the 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.

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

It has to be noticed that the definition of personal data goes beyond the common use in which the term personal data might apply to several types of data, which make it able to identify a natural person. Court staff 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.

Court staff 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 the combination of the name with other identifiers.

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 are

[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.

personal data and falls under the data protection rules.

3.3. Pseudonymisation

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 ensures 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 the Directive and by the GDPR contributes to harmonise the level of data protection between Member States. Court staff would benefit of this consistency when processing sensitive personal data in their daily activities.

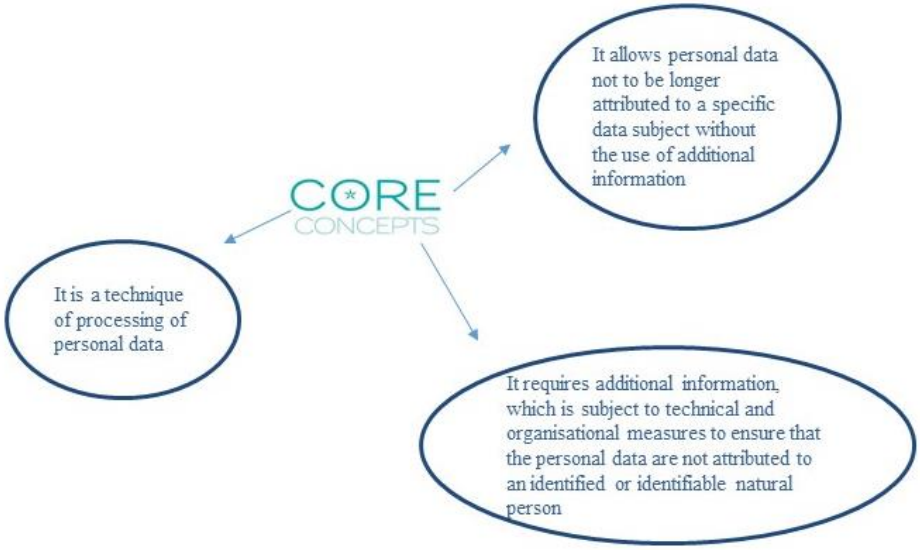
Directive 2016/680	***GDPR***
Art. 3 sec. 5	Art. 4 sec. 5
Pseudonymisation means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational	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 organizational

This project is funded by the 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.

measures to ensure that the personal data are not attributed to an identified or identifiable natural person.	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.

Core concepts



In particular

- Pseudonymisation is a "processing activity" that makes data no longer attributable to a specific 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.

- If pseudonymisation process is applied by court staff, they do not have to provide data subjects with rights to access, rectification, erasure or data portability
- 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[8]
- Technical and organisational measures are provided in order to secure non-attribution to a single identified or identifiable natural person
- 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

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 are 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

[8] Any encrypted data is pseudonymised data (encrypted databases, encrypted communication, encryption used for archiving purposes etc.)

This project is funded by the 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 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 external hack, the likelihood that someone within the sender's organization - 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 data protection rules. 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

This project is funded by the 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 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.

Recommendation

Court staff has to pay special attention on pseudonymisation techniques implementation. Even if no guidance on pseudonymisation has been released by the European Legislator yet, court staff 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. Court staff has to follow the willingness of the European legislator on data protection that 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 types of data

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

The aim of this section is to contribute to an in-depth and accurate knowledge of the meaning of the issues surrounding the concept and types of "sensitive personal data" under the GDPR and the Directive to deepen the expertise of the court staff.

This project is funded by the 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 homogeneity of the definitions of "sensitive personal data" provided by the Directive and by the GDPR contributes to harmonise the level of data protection between Member States. Court staff would benefit from this consistency when processing sensitive personal data in their daily activities.

Directive 2016/680	***GDPR***
Art. 10 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.	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 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 sensitive personal data. It has to be noticed that while GDPR provides for general rules on data protection, the Directive specifically applies to the protection of personal data in the criminal law context. Nevertheless, the basis of the "sensitive personal data" concept is absolutely the same.

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").

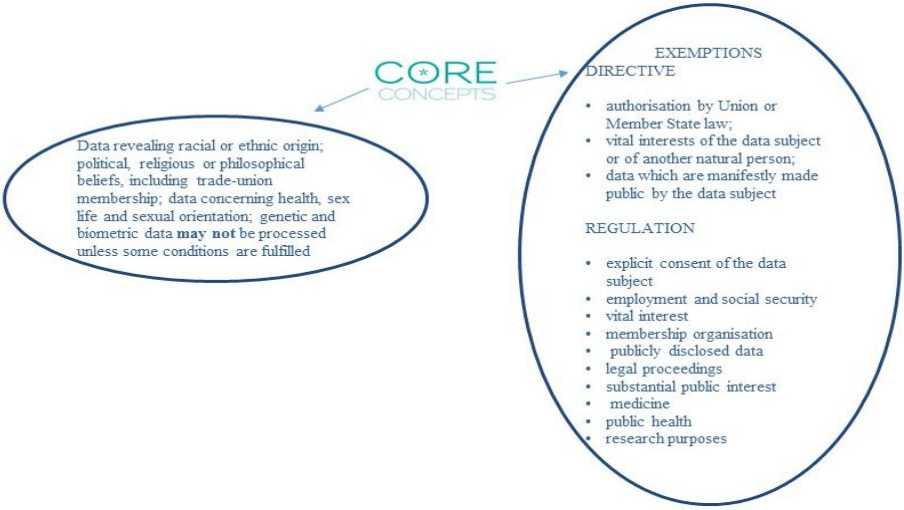
In other words, when processing sensitive personal data, judiciary needs to identify different conditions

• 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.

Core concepts



In particular

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

This project is funded by the 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 revealed 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 expenses 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

The most relevant exemption from the prohibition that applies to court staff is set in Art. 9, para 2 lit. f (legal proceedings):

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

Where the aforementioned is not applicable the following exemptions may apply, when court staff acts on behalf of data controller or processors or as data subjects:

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

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

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

Explicit consent of the data subject (Art. 9, Para 2 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.

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 the European Union or the Member State law provide that the prohibition may not be lifted by the data subject 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.

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.

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 European Union or the Member State law. Such legislation should be proportionate to the aim pursued, should respect the essence of the right to

This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this 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 and should provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

Other exemptions are related to the public health, medicine purposes, vital interest, membership organisation. However, these exemptions are not relevant to the court staff daily activities and therefore not part of the current guidelines.

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

- authorization by the European Union or the Member State law
- vital interests of the data subject or of another natural person
- data manifestly made public by the data subject

Data revealing criminal convictions (Art. 10 GDPR)

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.

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

This project is funded by the 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.

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".[9]

Relevant cases

Source: European Court of Human Rights, Press Unit, *Factsheet- Personal data protection*. April 2018[10]:

- Collection of fingerprints records:
  Eur. Court of HR, M.K. v. France, judgment of 18 April 2013, application no. 19522/09[11]
- Collection of health data:

Eur. Court of HR, L.H. v Latvia, judgment of 29 April 2014, application no. 52019/07[12];

Recommendation

Members of courts staff in their daily work activities have to 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

[9] See Voigt/von dem Bussche, *The Eu General Data Protection Regulation (GDPR). A practical Guide*, Springer International Publishing AG 2017.
[10] https://www.echr.coe.int/Documents/FS_Data_ENG.pdf
[11] http://hudoc.echr.coe.int/eng#{%22ecli%22:[%22ECLI:CE:ECHR:2013:0418JUD001952209%22]}
[12] 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.

reason court staff 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 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.

Legal background

The term "processing" is very broad both in the GDPR and 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

This project is funded by the 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.

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 contributes to harmonize level of data protection between Member States. Court staff would benefit of this consistency when processing personal data in their daily activities.

Directive 2016/680	***GDPR***
Art. 3 no. 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, organization, 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 para. 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, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

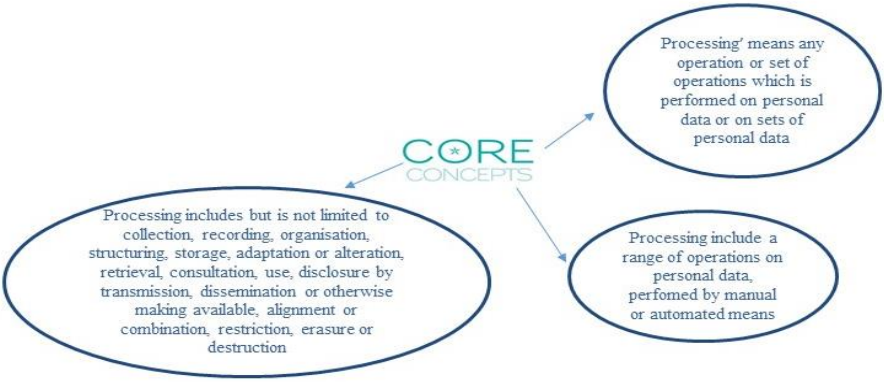
This project is funded by the EU. This deliverable has been produced with the financial support of the Justice Programme (2014-2020) of the European Union. The contents of this leaflet are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

Art. 3 no. 3 Restriction of processing' means the marking of stored personal data with the aim of limiting their processing in the future. Art. 3 no. 4 Profiling means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements.	

The Directive and the GDPR include other provisions related to personal data processing which are considered in different chapters of these Guidelines. 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 court staff 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 authorises associations and other bodies representing categories of controllers or processors to prepare codes of conduct, or amend or extend such codes. The collection of personal data occurs in many cases: in the process of administering legal claims, that have been filed, during the investigative phase and within the process about parties of the proceedings, about the suspect of a crime, about the witnesses, just for giving some examples. The data collection might be

This project is funded by the 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.

particularly relevant in case of gathering physical items that contain potential evidence (such as signed documents, fingerprints, DNA, voice interceptions, etc.).

Recording and storage

Having trace of processing activities is considered vital: a lot of data is collected as part of court staff daily activities, and it is of paramount importance to maintain a record of processing activities in order to ensure the lawfulness of the processing and the protection of the data subject's rights and freedoms. The GDPR strengthens the importance of maintaining a record of the data processing activities performed by data controllers. According to Article 30 of the GDPR, the data controllers (and data processors) have to implement records of their processing activities that should permit (if validly maintained) to prove compliant with the GDPR. This provision should apply to the judicial sector in order to have a valid chain of data processing activities.

Storage is one of the latest stages in the data processing cycle, where data is held for future use. This step allows quick access and retrieval of the processed information. In particular, court staff 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

This project is funded by the 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.

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 the court staff, which supports the judicial authority and secures the fulfilment of the obligations to which the data controller is subject to.

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. Court staff 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 takes place when the data subject exercise 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.

This project is funded by the 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.

Use, alignment or combination

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

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

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

Disclosure by transmission

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

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

According to Recital 83 of the 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.

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 or posting personal data on a web page.

This project is funded by the 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.

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

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

This project is funded by the 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. Lawfulness of processing

4.1. Article 6 of the GDPR

The basis for lawfulness of processing within the operations of court staff can largely be related to assessment regarding the judiciary as a whole. The court acts as a public body within its authority and jurisdiction. Therefore, the main basis for lawfulness of personal data processing through the court and its court staff can be seen in Article 6 para. 1 lit. c and lit. e GDPR.[13] The particular distinction between application of the legal basis pursuant to lit. c (compliance with a legal obligation) and lit. e (performance of a task carried out in the public interest or in the exercise of official authority) is subject to specific parameters of the particular data processing activity. The lawfulness of processing through the court staff, considering the broad understanding of this term, derives from the legal basis of processing applicable to the operations of the controller, i.e. the court. The primary relationship between the court staff and the court is based on an employment contract, which leads to the application of the regime under Article 29 GDPR (person acting under the authority of the controller or of the processor).

Compliance with a legal obligation to which the controller is subject pursuant to Article 6 para. 1 lit. c GDPR is to be considered as valid legal basis for activities of the court staff that are based on specifically formulated obligations derived directly from a legal provision that constitutes the

[13] Heinrich Amadeus Wolff and Stefan Brink, *Beck'scher Online-Kommentar Datenschutzrecht* (24. Edition, CH Beck München 2018) Art. 6, Rn. 35, first sentence.

This project is funded by the 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.

necessity of personal data processing.[14] On the other hand, Article 6 para. 1 lit. e GDPR is applicable as legal basis for processing pursuant to legal provisions that constitute authorization for personal data processing rather than concrete obligation.[15] The core of this basis is the necessity for performance of a task carried out in the public interest or in the exercise of official authority. It is particularly the exercise of official authority that aims at lawfulness of personal data processing during the performance of judicial authority vested in the court through respective national constitution and laws. The basis is limited by the criterion of necessity, which in this case is to be interpreted rather as proportionality of the measure relative to its alternatives.[16] The specific requirements for processing and other measures to ensure lawful and fair processing pursuant to Article 6 para. 1 lit. c and lit. e GDPR may differ among Member States, as they may be provided through national legislation (Article 6 para. 2 GDPR).

The other legal basis available under Article 6 GDPR are less likely to be applicable to the performance of the main tasks of the judiciary, they should, however, not be omitted with regard to some supporting or auxiliary roles of the court staff. In case of processing based on informed, freely given and revocable consent of the data subject to the processing of his or her personal data for one or more specific purposes (Article 6 para. 1 lit. a and Article 7 GDPR), it must be noted, that consent between employer

[14] Wolff and Brink (n 9) Art. 6, Rn. 34; Boris P Paal and others, *Datenschutz-Grundverordnung: DS-GVO* (CHBeck 2017) Art. 6, Rn. 18; Christopher Kuner, Lee A Bygrave and Christopher Docksey, 'Draft Commentaries on 10 GDPR Articles (from Commentary on the EU General Data Protection Regulation, OUP 2019)', *Commentary on the EU General Data Protection Regulation* (Oxford University Press 2019) 44 <https://works.bepress.com/christopher-kuner/1/>.
[15] Wolff and Brink (n 9) Art. 6, Rn. 35, last sentence.
[16] Paal and others (n 10) Art. 6, Rn. 23.

This project is funded by the 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.

(court) and employees (court staff) is fundamentally affected by the unequal legal relationship of these parties, which jeopardizes the free aspects of such consent.[17] For this reason, consent should be regarded as secondary legal basis and applicable only to processing not related to the performance of work tasks of the court staff members. The application of Article 6 para. 1 lit. b GDPR (processing is necessary for the performance of a contract) can be relevant with regard to personal data required from the court personnel for the management of the employment relationship. The term "performance" should be interpreted in accordance with terminology of the European law, hereby including also the duty to perform, side obligations and obligations to consider related to the employment contract.[18] Legal basis pursuant to Article 6 para. 1 lit. GDPR also applies to pre-contract communication and negotiation, e.g. personal data processing related to work applications, as they constitute necessary steps at the request of the data subject prior to entering into the contract. Article 6 para. 1 lit. f GDPR (processing necessary for the purposes of the legitimate interests pursued by the controller or by a third party) may apply to prolonged storage of personal data about former members of court staff. However, it needs to be noted, that such legal basis must be balanced against the interests or fundamental rights and freedoms of the data subject and needs to be therefore interpreted in a strict sense.

4.2. Article 9 of the GDPR

With respect to processing of special categories of personal data pursuant to Article 9 of the GDPR should be noted the exception included under para.

[17] Paal and others (n 10) Art. 6, Rn. 12; Wolff and Brink (n 9) Art. 6, Rn. 21.
[18] Wolff and Brink (n 9) Art. 6, Rn. 31.

This project is funded by the 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 lit. f for processing within the scope of judicial capacity of the given court. The particular landscape of judicial capacity depends on specific national legislation and organization of judicial system, as well as specific role and functions of the given court in such a national system. 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.[19]

The court staff does also process special categories of personal data related to other members of the court personnel within its auxiliary functions. These processing should be primarily connected to the administrative aspects of the internal organization of the court, e.g. management of human resources and their respective suitability for various roles within the court personnel hierarchy. Such processing should be covered by exception under Article 9 para. 2 lit. b of the GDPR, aimed at processing 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 within the legal bounds and with appropriate safeguards for the fundamental rights and the interests of the data subject in place.

4.3. Article 8 of the Directive

The lawfulness of processing under the Directive 2016/680 is closely linked with the specific subject-matter of this legislation. The Member States are obliged to implement the Directive in a way, that sets as lawful only a processing necessary for the performance of the task by the competent

[19] Paal and others (n 10). 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.

authority 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 (Article 8 para. 1 of the Directive). The assessment of lawfulness shall be therefore closely bound to the interpretation of the appropriate national legislation that sets the objective for the processing, indicated the scope of personal data affected and defines the purposes of such processing.

The Directive also takes into account the processing of special categories of personal data, where one of the exceptions under Article 10 should exist in order for the processing to be lawful.

5. Data subject 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	Art. 18	Art. 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.

processing		
Right to data portability	Art. 20	N/A
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[20] (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):

[20] In the context of judiciary, thus court staff in supporting the administration of the data subjects' requests, the most relevant situation will be the one where the holder of the parental responsibilities exercise these rights on behalf of the child.

This project is funded by the 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.

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 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.

This project is funded by the 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 addition, the data controller must provide further details on the specific circumstances of data processing in accordance with the respective Paragraph 2 of the mentioned articles.[21]

→ The rights to information pursuant to Articles 13 and 14 implement the principle of transparency, which can be applied to the processing by the court as a whole, rather than specifically to court staff operations. 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.[22]

- **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

[21] To the background of the details to be provided and the right of information in general see Article 29 Working party, Guidelines on transparency under Regulation 2016/679, WP260, in particular p. 31-35.
[22] 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.

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 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.

→ Such a limitation of the right of access to processed personal data must be assessed with proportional balancing of the fundamental right of the data subject and potential risks to the independence of justice. Its performance towards auxiliary court staff activities is less likely to be restricted, if compared with processing related to court files.

- **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.

→ The right to rectification pursuant to Article 16 plays important role, if the erroneous or incomplete data could negatively affect the court proceeding. This right should the data subject be already able to routinely exercise with regard to mistakes in registries administered by the courts.

This project is funded by the 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 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 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).

This project is funded by the 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 court staff, 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. 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). Even in this case, however, it must be carefully considered whether the files can also be retained without the personal data. 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

This project is funded by the 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.

- 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 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.[23] 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[24], 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 court staff, it should be noted that this right are not relevant to current form of judiciary arrangement. In general, it 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).

[23] See Article 29 Data Protection Working Party, Guidelines on the right to data portability, WP242, adopted on 5 April 2017, p. 15.
[24] 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.

- **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 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).

→ The facilitation of the exercise of the right to object should be aligned with a more general right to complaint, however, application of this right should not lead to obstacles in the court proceeding.

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 above). In addition, the data subject rights in the Directive can be further restricted.

This project is funded by the 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.

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; 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

This project is funded by the 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.

corrected by the courts when evidence was illegally obtained (for instance, because a warrant is missing). Such sanctions may be, for instance, excluding 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
Requires from the data controller to demonstrate a high degree of transparency 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 has the information	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); The Directive does not distinguish whether the data were collected

This project is funded by the 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. 13, para. 4 / Art. 14, para. 5 lit. a); Further limitations are only applicable where the data were not collected directly from the data subject (Art. 14) • 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); • where obtaining or disclosure is expressly laid down by Union or Member State law to which the controller is subject (Art. 14,	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.[25] 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 prosecution, it is not always possible to make the data subject aware of the processing.[26] However, Art. 13, para. 2 of the Directive provides for the direct supply of specific information to the

[25] 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.
[26] *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.

para. 5 lit. c) • where the personal data must remain confidential subject to an obligation of professional secrecy (Art. 14, para. 5 lit. d).	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.

6. Rights and obligations of data controllers & data processors

As a starting point for the specific obligations and as a central common instrument of both the GDPR and the Directive 2016/680, the risk-based approach is to be emphasised. What this means is that all circumstances of

This project is funded by the 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 processing must always be guided by the degree of objective risks for the data subject and their likelihood of occurrence.

Since a distinction is made between the position of the data controller and that of the data processor with regard to the rights and obligations, it is necessary to determine the respective position on the basis of the actual circumstances for each data processing. A data controller is legally defined as the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data (Art. 4, sec. 7 GDPR / Art. 3, sec. 8 of the Directive). In contrast, a data processor is legally defined as a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller (Art. 4, sec. 8 / Art. 3, sec. 9 of the Directive).

If data processing by judges takes place for the purpose of fulfilling the judicial tasks, there is, as a consequence of judicial independence, a sovereign activity without instruction obligation. This assessment is in line with the GDPR's emphasis on judicial independence. Nevertheless, an abstract categorisation of each individual processing in the judicial field cannot be made across-the-board due to the particularities of the Member States' systems and the different competences and responsibilities of judges and prosecutors. Accordingly, a determination as to whether the court as 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.

whole or a single judge is to be regarded independently as data controller is dependent on national regulations and the circumstances of the individual case.

Court staff, as personnel of a court, does not represent a specific data processing entity. Its role and obligations are derived from the role and obligations of the court, as the entity to which the members of court staff are legally bound by contractual links of employment.

Data controller obligation	GDPR	Directive 2016/680
Data protection by design	Art. 25	Art. 20
Data protection by default	Art. 25	Art. 20
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

Table 6.1 Overview of data controller obligations in Directive 2016/680 vs the GDPR.

6.1. Obligations

Protection of personal data represents a legal regime aimed at regulating the broad scope of activities that constitute a processing of personal data

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

through risk-based rules intended to incorporate considerations of negative effects that such processing might have on the natural persons, who are subjects identified through the data. The obligations are therefore closely linked to general principle of accountability, i.e. to the ability of the data controller or data processor to adequately assess the particular setting, apply a measure or response appropriate to the risks presented to the affected natural persons and demonstrate this process to supervisory authority. The obligations and measures discussed in this section need to be applied on a case-by-case basis with consideration of specific national requirements for judiciary pursuant to Recital 20 GDPR and the Directive, particular setting of the given court and critical assessment of risks for data subjects.

Subject primarily responsible for adequate internal structure and operations in compliance with personal data protection requirements is the court, represented by its administrative body and statutory chairman (president of the court or other functionally similar position). The members of the court staff should be adequately informed and educated about their duties and appropriate internal processes with regard to processing of personal data during their work tasks and supervision of compliance should be incorporated into the broader structure of employee hierarchy and supervision. Such process also includes drafting or modification of the internal documents and directives in order to include personal data protection and cybersecurity policy.

Similar to all controllers, the data flows and operations representing processing of personal data should be conducted in organized manner, appropriately documented and the documentation kept up to date in order to provide the court administration with usable overview of personal data

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

processing landscape enabling risk assessment and implementation of adequate measures.

Given the specific role of courts as publically established bodies for dispute resolution, the internal framework of operations, functions and duties is generally well developed and the rather rigid structure, compared to commercial subjects, allows for stable structure and data flows specified through internal documents and plans based on legislative definition of the courts role as public judicial body. Rather than building of personal data protection framework, the courts are faced with assessment of their established practices to confirm the compliance of their processes with the updated requirements and to identify potentially risky operations that should receive increased attention.

These instances can be identified primarily based on criteria for personal data processing risk assessment,[27] which include e.g. size of the processed personal data evidence, relative sensitivity of the personal data, accessibility of the evidence, accuracy of the personal data, or forms of routine operations affecting the evidence. Notwithstanding the organizational specifics of each court, these instances can occur particularly in relation to log of the contents and manipulations with the court files, archiving of the court files, evidence of the correspondence, evidence of the presence at the court premises, database of the access authorization, or administration of the court information systems. Areas with higher risk of negative impact on rights and freedoms of natural persons require stricter compliance with

[27] See e.g. scoring criteria for severity of personal data breach provided by ENISA. ENISA, 'Recommendations for a Methodology of the Assessment of Severity of Personal Data Breaches' (20 December 2013) <https://www.enisa.europa.eu/publications/dbn-severity> accessed 7 February 2018. 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.

obligations and more complex measures to be implemented, in order to provide an adequate level of protection.

In the GDPR and the Directive are for this purpose articulated two specific requirements; data protection by design and data protection by default. The former applies to implementation of new work-flow routines, e.g. adoption of e-justice system of case file manipulation process. In such instances the aspects of data protection need to be considered from the onset and during all stages of the project and its implementation. The data protection by default will present a challenge, especially when developing an IT system to be applied in the court setting, as the latter needs to be flexible in order to accommodate broad variety of tasks that involve pursuit of evidence, collection, analysis and other forms of processing of various personal data with the aim of resolving the ensued dispute, while at the same time observes the principles of the GDPR and the Directive – i.e data minimization, purpose limitation, .

The requirement of data protection by default needs to be taken into consideration with respect to access authorisation and data storage.

It cannot be excluded that some court activities may be subject to systematic data protection impact assessment pursuant to Art. 35 GDPR or Art. 27 of the Directive. Such assessment requirement may apply to the court as a whole, reflecting its capacity to process special categories of data on large scale as part of its main activities (Article 35 para. 3 lit. b GDPR). Similarly a particular impact assessment may be necessary for the court information systems. Such instances would, however, be coordinated either with the provider of the system and limited to impact of the specific setting as part of the court operations or through judiciary as a whole. An instance where

This project is funded by the 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 activities of court staff would establish an obligation of impact assessment seems highly unlikely.

Similarly the specific obligation of mandatory appointment of data protection officer (DPO) is a matter relevant beyond the activities of court staff and highly dependent on particular national regulatory framework. Art. 37 para. 1 lit. a GDPR and Art. 32 para. 1 of the Directive specifically exclude from the mandatory obligation courts acting in their judicial capacity. However, despite this exception, it must be considered, if the judicial capacity encompasses all activities of the court that represent personal data processing. Such interpretation is not unified between the Member States. Given the differences in structural approaches to judiciary, it is unsuitable to be interpreted on the level of European law.

6.2. Organisational and technical measures

Crucial focus of personal data protection with regard to court staff activities should be on adequacy of the implemented organisational and technical measures. This, however, cannot be seen as independent from the broader organizational framework of the court and its other requirements. As noted by Emery and De Santis; the proper setting of court management is a rather complex matter with many conflicting goals, functions and values.[28]

6.2.1. Organisational measures

Nevertheless, from the organizational perspective should the measures required by personal data protection include dutiful management of access authorization, proper chain of delegation within the court hierarchy with

[28] Yves Emery and Lorenzo De Santis, 'What Kind of Justice Today? Expectations Of "Good Justice", Convergences And Divergences Between Managerial And Judicial Actors And How They Fit Within Management-Oriented Values' (2014) 6 International Journal for Court Administration <http://www.iacajournal.org/articles/abstract/10.18352/ijca.118/> accessed 28 January 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.

clearly defined roles and responsibilities, adequate or regular employee training and education, manuals and support in case of incidents or errors, internal audit and monitoring structures, cultivation of awareness to threats and security routines throughout the court work environment. There is no specific benchmark for these measures as their concrete form needs to be adjusted to the specific setting, structure and potential risk related to the operations of the court staff in the particular court.

There are also requirements set by GDPR and the Directive that the courts perform by default in accordance with their specific obligations and regulations connected to their judiciary competence. An example may be the adequate documentation of personal data processing activities, which has its established format in the court routine set by internal regulation or national legislation.

The particularities of requirements set in Article 30 GDPR and Art. 24 (record keeping) and 25 (logging of automated processes) of the Directive are bound to national approach to supervision of the personal data processing within the judiciary. In this regard, the records accessible to external supervisory or administrative bodies should avoid granularity that would allow identification of particular cases, data subjects or activities, as such detailed documentation is likely to present additional security risk as well as risk for the impartiality and independence of the court and the judge.

6.2.2. Technical measures

The technical requirements of personal data protection are primarily bound to the security of processing. As such, the matter cannot be fully separated from the general requirements on safety and security in the court environment. For this reason assessments and guidelines for court security design and architecture are a valuable input for considerations of adequate

This project is funded by the 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.

measures for secure personal data processing by the court staff. With respect to protection of personal data, a particular attention must be devoted to implemented ICT technologies. Security of personal data protection is in this regard an aspect of broader cybersecurity requirements, which is aimed at securing confidentiality, integrity and availability of the processed data.

The starting point for assessment of the adequacy of the technical measures is therefore their capacity to appropriately mitigate the risks related to breaches of confidentiality (e.g. access to data from personal insolvency registry, list of secret witnesses, expert witness documentation in sensitive cases), integrity (e.g. modification of the court file metadata, changes in dates, names, wrong attachment of files to cases, changes in operation logs) or availability (e.g. ransomware attack encrypting the court databases, DDoS attack on court electronic communication servers, deletion of electronic court files) of the given set of processed personal data.

Particularly vulnerable may be internal operations with large databases of personal data depending or being managed with the help of ICT systems (e.g. HR database of court staff, coordination and distribution of internal tasks, log of court files contents, operations with digitalized court files).

Beyond the already mentioned issues of security comes into question the continuously increasing ubiquity of dependence on ICT devices and their functions, which manifests also in the court environment. One side of the coin is the progress in all Member States towards implementation of some e-justice features in the judicial operations. Work of the court staff requires operating with information systems, computer programs, internet

This project is funded by the 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.

connection and digital communication tools.[29] Considerations need to be given to the potential impacts of the established connectivity of court systems processing data related to court files and other sensitive information. There should therefore be a systematic coordination and integration of applied measures across the judiciary in general and across the departments of the court in particular, in order to provide for secure communication, interoperability and efficiency of the adopted measures.

Another factor of the connectivity is the use of personal devices by the court staff or other visitors to the court premises. Unintentional vulnerabilities may come from lenient wireless connection security policy at the court premises; consciously may the mobile devices be used for unauthorized record, duplication or circulation of internal documents containing sensitive personal data.

The importance of adequate cybersecurity measures is further underpinned by the eventual impact of court activities on high-stake situations. This applies particularly to the criminal proceedings, but even in other cases the court may play crucial role in politically or personally highly sensitive matters.

As the court staff, while assisting the judge, managing the correspondence and court files, communicating with the witnesses and other stakeholders, searching and analysing the data available in the internal information systems and performing other task, operates with case files and other court documents in their full-content version and access to the information systems of the court. Therefore they have access to a broad spectrum of detailed personal data about clearly identified data subjects. Of particular

[29] See Use of information technology in European courts - CEPEJ, Council of Europe, p. 17-18.

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

sensitivity may be some forms of evidence, e.g. expert witness reports in medical malpractice cases (often including photographic documentation or intimate personal data related to personal health), evidence in cases related to financial compensation for victims of violent or sexual criminal offences, personal insolvency registry entries and files, reports, evidence and transcripts from divorce proceedings, adoption proceedings, paternity determination proceedings, evidence related to certain types of insurance claims, identity of protected witnesses in whistle-blower cases, witness statements and evidence in antidiscrimination or employment disputes, as well as cases related to other forms of infringement into personality rights.

Particularly if the court information systems are shared with other courts, the personal data are indexed or in some other way include metadata structure for easier processing of the stored database of documents, this needs to be regarded as factors increasing the cybersecurity risks related to the processing of such personal data, as it increases the size of the database, simplifies the orientation and manipulation with its contents and opens new vectors for potential threat scenarios.

The court staff activities must therefore be considered with respect to threats of internal (or external) intentional (or accidental) access, manipulation or erasure of case relevant information that include personal data and the organisational and technical measures must be aimed to limit the possibility and impact, if such data breaches occur. At the same time, however, the court staff must retain an effective access to the data necessary for its performance of work duties.

In response to these risks, the court is obliged to have adequate protective measures in place, mitigating the identified risks to acceptable level. Such requirements are similarly set in national cybersecurity legislation (currently

This project is funded by the 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 minimal harmonisation through implementation of the Directive on security of network and information systems 2016/1148 and pursuant to guidelines and recommendations by the European Union Agency for Network and Information Security (ENISA)). Aside from above mentioned organisational measures, it is particularly the technical checks and balances incorporated in the court information system, but also the physical premises of the court, that create the boundaries for secure processing of personal data during the court staff activities. There are multiple sources of general recommendations and best practices for physical and cyber security that provide particular examples of technical solution available and adequate to various types of settings.

6.3. Reporting obligations

The obligations related to organisational and technical measures are aimed at prevention of unauthorized access and processing of processed personal data. Newly introduced general mandatory personal data breach notification obligation is focused on impact mitigation of such detrimental event. It is therefore a supplementary instrument to the security requirements under Article 32 GDPR, which should include among other aspects also an effective detection of personal data breaches.[30] There remains uncertainty about application of these obligations to the judiciary. This is largely because the interpretation of the notification obligation under Art. 33 of the GDPR or Art. 30 of the Directive is closely connected to quantification of the potential threat and the structure of supervision. The notification obligation lies with the controller. If the supervisory role is transferred to a specific body within the judiciary, the notification obligation should be towards this body. As such, particular communication platforms need to be established.

[30] Article 29 Data Protection Working Party, 'Guidelines on Personal Data Breach Notification' p. 6.

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

The assessment of the risk posed by the data breach is generally challenging, there are, however methodologies available, e.g. by ENISA.[31] Given the particular sensitivity of court operations, primary focus should, however, be on preventive measures, given that a data breach may indicate possible disruption of the court operations that may infringe upon e.g. the right to fair trial.

As a consequence, adequate procedures should be put in place in case of need for communication of data breach to the data subject, when the breach is likely to result in a high risk to her or his rights and freedoms pursuant to Art. 34 of the GDPR or Art. 31 of the Directive. Fulfilling this obligation is bound to protection of procedural rights and fairness of the trial. As the occurrence of data breach cannot be fully eliminated, there need to be adequate monitoring measures, reporting procedures and court staff training to minimize potential impact of such incident with timely response in organized and professional manner.

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. Court staff may need to participate in the transfer of personal data when legal assistance is requested by or from a third country. The requests may contain names, addresses, date and place of birth and other data of participants in the process in relation to which the transfer is necessary. When sending judicial

[31] See ENISA, 'Recommendations for a Methodology of the Assessment of Severity of Personal Data Breaches' (20 December 2013) <https://www.enisa.europa.eu/publications/dbn-severity> accessed 19 April 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.

acts for recognition by the other country, data about the parties to the case and criminal convictions and offences may be transferred.

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. Moreover, the exercise of rights of the individuals and the possibilities to pursue complaints and conduct investigations in third countries regarding data protection may be hindered. That is why transfers to third countries are permitted in four cases (with regard to court staff):

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 CJEU[32], 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[33], 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. Court staff 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

[32] ECLI:EU:C:2015:650[GC] (Schrems), para 74.
[33] Adequacy Referential (updated), Article 29 Data Protection Working Party, Adopted on 28 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.

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. This case is important for court staff, as many countries have signed mutual legal assistance treaties. In most situations transfers executed by court staff will be based on these grounds. According to Art. 48 of the GDPR, 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 that are relevant to court staff may be legally binding and enforceable instruments or (with authorisation from a supervisory body) provisions in administrative arrangements between public authorities or bodies.

4) Specific situations – the GDPR permits transfers even if one of the already mentioned cases is not present. The most relevant to court staff 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. There is low probability that court staff 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.

This project is funded by the 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.

As some structures within a court may perform tasks under Art. 1 of Directive 680/2016, court staff 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;
- 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

This project is funded by the 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.

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 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

This project is funded by the 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 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 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.

Court Staff 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.

Court Staff 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.

This project is funded by the 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. Legal remedies available to data subjects

8.1. Supervisory authority

The structure of personal data protection supervision in judiciary is relevant to demonstration of compliance with above described obligations. Supervision by data protection authority outside of judiciary may challenge the independence of the judiciary. Particular supervisory structure in the Member State is connected to the structure and administration of the judiciary, particularly to the existence of judicial council or other central administrative agency.

8.2. Administrative fines

There is a harmonized structure of administrative fines for breaches of compliance with the data protection regime under GDPR (Articles 83 and 84 GDPR). However, as the judiciary and thereby also the court staff have specific position in this framework pursuant to Recital 20, the applicability of administrative sanction is likely to be modified through the specific national legislation. Furthermore, the structure of supervisory authority over personal data processing by the judiciary is also likely to reflect upon the setting and enforcement of administrative fines under this regime.

The person finally responsible for compliance with the data protection regulation by the court is in most cases the court statutory body, i.e. the court president, chairman or magistrate. Despite the theoretically applicable draconic administrative fines for non-compliance (depending on the type of infringements, the upper limit of the administrative fine is set to 10,000,000 EUR or even 20,000,000 EUR (Article 83 para. 4-6 GDPR). The fine as percentage of worldwide turnover is not relevant in the context of judiciary bodies), it is likely to presume, that these forms of sanctions shall function

This project is funded by the 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.

merely as motivation for court administration to ensure compliance, rather than applied instrument of its enforcement.

At the same time, it should be noted, that excessive formal pursuit of supervisory sanctioning capacity over a court could lead to interference with its judicial independence and impede the effective functioning of the court in its judicial capacity, which is neither in accordance with the requirements for administrative fines under Art. 83 GDPR as interpreted in Recitals 148-151 GDPR nor with the concept of personal data protection framework in general.

The Directive 2016/680 does not prescribe specific form or rules for administrative penalties and delegates the capacity to set the rules for effective, proportionate and dissuasive penalties to the Member States (Article 57 Directive).

8.3. Legal remedies available to data subjects

1) Right to lodge a complaint with a supervisory authority

GDPR

When the data subject considers that the processed personal data relating to him or her may be infringing upon the GDPR, 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. [see Art. 77 para. 1 GDPR; Art. 52 para. 1 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.

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 to another supervisor 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. [see Art. 77 para. 2 GDPR; Art. 52 para. 2-4 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 GDPR]
- when personal data have not been obtained from the data subject [Art 14 para. 2 lit. e GDPR]
- when the controller does not take action on a request by the data subject [Art. 12 para .3 GDPR]

Directive 2016/680

The same provisions apply in cases of infringement of data subject's rights under the Directive.

Measures for implementation/compliance

This provision does not interact with the work of court staff as it provides for procedures before the supervisory authority.

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 shall not be competent to supervise processing operations of courts acting

This project is funded by the 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 their judicial capacity. For processing that is performed in another capacity (as an employer for instance) the supervisory authority shall be competent.

Additionally, there is also the possibility, enshrined in Recital 20 of the GDPR, that Member States "*should be possible to entrust supervision of such data processing operations to specific bodies within the judicial system of the Member State, which should, in particular ensure compliance with the rules of this Regulation, enhance awareness among members of the judiciary of their obligations under this Regulation and handle complaints in relation to such data processing operations*". In Recital 80 the Directive reflects the concept of Recital 20 of the GDPR, without explicitly outlining this possibility. What should be noted in relation to the various court staff positions, is that an assessment should be made in any case in order to decide, whether the processing undertaken by a particular court staff representative constitutes a part of the exercise of the judicial capacity. If the processing is performed for the mere administrative purposes then the supervisory authority will be competent.

2) Right to an effective judicial remedy against a supervisory authority GDPR

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.

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

The exercise of such judicial remedy does not prejudice the availability to the data subject of any other administrative or non-judicial remedy.

[see Art. 78 GDPR; Art. 53 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. [see Art. 78 para. 4 GDPR]

Directive 2016/680

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.

Measures for implementation/compliance

There are no special measures to be taken by court staff in the implementation of this provision.

It shall, however be kept in mind that such a claim may be commenced by a not-for-profit organisation on behalf of the data subject whose rights have been infringed. [see Art. 80 GDPR; Art. 55 Directive]

3) Right to an effective judicial remedy against a data controller or processor

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.

The data subject is given the right to effective judicial remedy in cases where the data subject decides to take judicial measures for an infringement with his rights regarding his personal data.

When the data subject considers that the processing personal data relating to him or her may be infringing upon the GDPR, 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 GDPR but where controller or processor do not have an establishment in a Member State, the establishment of the representative designated under Art. 27 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 Member State acting in the exercise of its public powers. [see Art. 79 GDPR; Art. 54 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. [see Art 12 para. 3 GDPR]

Directive 2016/680

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

This project is funded by the 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.

Measures for implementation/compliance

There are no special measures to be taken by court staff in the implementation of this provision.

It shall, however be kept in mind that such a claim may be commenced by a not-for-profit organisation on behalf of the data subject whose rights have been infringed. [see Art. 80 GDPR; Art. 55 Directive]

4) Right to compensation and liability

GDPR

Data subjects have the right to full and effective compensation for material or non-material damage suffered as a result of infringement of the GDPR. [see Art. 82 GDPR, Rec. 146 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 GDPR 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. [see Art. 82 and 79 GDPR, Rec. 147 GDPR; Art. 56 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.

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:

- it has not complied with the obligations specifically addressed to processors under GDPR 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 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 lodge the complaint on his or her behalf. Such entity must be duly constituted and have public-interest statutory objectives. [Art. 80 GDPR]

Directive 2016/680

The same right exists for infringement with Directive or national provisions implementing the Directive. [Art. 56 Directive, Rec. 88 Directive] However, the provisions under the GDPR are much more extensive than the more general and simple provision found in 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.

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

Measures for implementation/compliance

There are no special measures to be taken by court staff in the implementation of this provision.

5) Right to be represented

GDPR

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. [see Art. 80 GDPR; Art. 55 Directive]

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.

A regulation is provided for both the legal instruments as well as the requirements which the mandated body shall fulfil.

However, the GDPR additionally allows national legislation that permits 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 GDPR have been infringed as a result of the processing.

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 Directive)

Measures for implementation/compliance

There are no special measures to be taken by court staff in the implementation of this provision.

8.4. Procedure for complaints and requests

There is a likely conflict between the full exercise of the rights of data subject and the independence of judiciary and performance of judicial capacity by the court. For this purpose the Articles 23 of the GDPR as well as 15 para. 1 of the Directive (further interpreted through Recital 44 and following) permit appropriate restriction of the rights through national legislative measure. Such restriction must constitute necessary and proportionate measure in a democratic society to safeguard the protection of judicial independence and judicial proceedings and the enforcement of legal claims. At the same time, the essence of fundamental rights and freedoms of the data subject must be respected. Of particular relevance is therefore the specific procedure that allows exercise of rights of the data subject. Suitable approach needs to be established to allow effective exercise

This project is funded by the 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.

of the right to rectification pursuant to Article 16 GDPR and Article 16 of the Directive, which plays important role, if the erroneous or incomplete data could negatively affect the court proceeding. However, this right should the data subject be already able to routinely exercise with regard to mistakes in registries administered by the courts; therefore the adequate routine should be mostly well established.

The facilitation of the exercise of the right to object pursuant to Article 21 GDPR is in most regards a specific form of a more general right to complaint, which is common part of the rules of court proceedings and has mostly informal proceeding without an authoritative decision being issued, which prevents from the complaint being used for obstacles in the court proceeding.

Rights with a strong potential for creating obstacles to court proceeding are the right to erasure pursuant to Article 17 GDPR or Article 16 of the Directive and right to restriction of processing pursuant to Article 18 GDPR. The procedural exercise of these rights is a matter of specific national legislation, the implications of formal as well as informal procedure should, however, be duly considered.

This project is funded by the 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. Appendix: Helpful literature

- CEPEJ, 'Study on the Functioning of Judicial Systems in the EU Member States. Facts and Figures from the CEPEJ 2012 -2014 Evaluation Exercise' <http://ec.europa.eu/justice/effective-justice/files/cepj_study_scoreboard_2014_en.pdf>
- Emery Y and Santis LD, 'What Kind of Justice Today? Expectations Of "Good Justice", Convergences And Divergences Between Managerial And Judicial Actors And How They Fit Within Management-Oriented Values' (2014) 6 International Journal for Court Administration <http://www.iacajournal.org/articles/abstract/10.18352/ijca.118/>
- ENISA, 'Recommendations for a Methodology of the Assessment of Severity of Personal Data Breaches' (20 December 2013) <https://www.enisa.europa.eu/publications/dbn-severity>
- European Commission for the Efficiency of Justice, 'Use of Information Technology in European Courts - CEPEJ Study No. 24' <http://www.coe.int/t/dghl/cooperation/cepej/evaluation/2016/publication/CEPEJ%20Study%2024%20-%20IT%20report%20EN%20web.pdf>
- INFORM Deliverable 2.1 – Review report on the GDPR for the judiciary
- INFORM Deliverable 2.2 – Review report on the Directive for 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.

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
- Kuner C, Bygrave LA and Docksey C, 'Draft Commentaries on 10 GDPR Articles (from Commentary on the EU General Data Protection Regulation, OUP 2019)', Commentary on the EU General Data Protection Regulation (Oxford University Press 2019) <https://works.bepress.com/christopher-kuner/1/>
- Oertel RR and Goldschmidt PIB, 'The Training of Court Staff and Bailiffs at the European Union Level' in Directorate-General for Internal Policies of Union (ed), The Training of Judges and Legal Practitioners (European Parliament 2017) <http://www.europarl.europa.eu/RegData/etudes/IDAN/2017/583134/IPOL_IDA(2017)583134_EN.pdf>
- Paal BP and others, Datenschutz-Grundverordnung: DS-GVO (CHBeck 2017)
- 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

This project is funded by the 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.

Regulation (GDPR) – A Practical Guide, *Springer* – 2017
Wolff HA and Brink S, Beck'scher Online-Kommentar Datenschutzrecht (24. Edition, CH Beck München 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.