INTRODUCTION OF THE DATA PROTECTION REFORM TO THE JUDICIAL SYSTEM
INFORM

JUST-JTRA-EJTR-AG-2016
Action grants to support European judicial training
JUSTICE PROGRAMME
GA No. 763866

INtroduction of the data protection reFORM to the judicial system
INFORM

WP2 Data Protection regulatory review & training material elaboration

D2.5 Review report on Directive (EU) 2016/680 aimed at the legal practitioners

Lead partner: University of Wroclaw, Research Center on Legal and Economic Issues of Electronic Communication

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

Project co-funded by the European Commission within the JUST Programme		
Dissemination Level:		
PU	Public	X
CO	Confidential, only for members of the consortium (including the Commission Services)	
EU-RES	Classified Information: RESTREINT UE (Commission Decision 2005/444/EC)	
EU-CON	Classified Information: CONFIDENTIEL UE (Commission Decision 2005/444/EC)	
EU-SEC	Classified Information: SECRET UE (Commission Decision 2005/444/EC)	
Document version control:		
Version 1	Originated by: Damian Klimas, CBKE, University of Wroclaw	31/01/2018
Version 1	Reviewed by: Matthias Eichfeld, University of Göttingen	01/02/2018
Version 2	Updated by: Damian Klimas, CBKE, University of Wroclaw	02/02/2018
Version 2	Reviewed and updated by: George Dimitrov, Law and Internet Foundation	05/02/2018
Version 3	Updated by: Damian Klimas, CBKE, University of Wroclaw	13/02/2018
Version 4	Reviewed and updated by: Anna Zalesińska, Damian Klimas, CBKE, University of Wroclaw	19/04/2018
Version 4	Reviewed by: George Dimitrov, Desislava Krusteva, Law and Internet Foundation	23/04/2018

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

INFORM project

The INFORM project (Introduction of the data protection reform to the judicial system) is funded by the European Commission under the Justice Programme 2014-2020 with the primarily objective to train trainers for the judicial system. The goal of the project is to provide comprehensive and multidisciplinary understanding of the new EU General Data Protection Regulation (GDPR) and the new Directive (EU) 2016/680 through the development of high quality training materials, trained trainers in the field throughout all Member States and create a state-of-the-art e-Learning program. Moreover, the analytical activities of the INFORM project will examine the balance between personal data protection and the other fundamental rights in order to deepen the expertise of the professionals, especially when it comes to judges and lawyers. The project aims to reach the judiciary, legal practitioners and court staff using train-the-trainer approach.

During INFORM implementation, a Data Protection Trainers' network will be initiated. It will unite at least 180 persons from all over Europe with knowledge and skills. Apart from the trainers' network, the INFORM e-Learning programme will provide accessible and interactive training. The launched e-Learning platform will be promoted to the target groups, thus enabling them to self-improve their knowledge in the field.

INFORM implementation aims to improve knowledge, competences and attitudes to judiciary, legal practitioner and court staff rights and obligations pursuant to Directive (EU) 2016/680 and Directive (EU) 2016/680. Meanwhile they will be able to improve their capacity and skills in the services they provide.

The project team includes ten European partner organisations from leading universities and research centres in Bulgaria, Cyprus, the Czech Republic, France, Germany, Hungary, Italy, the Netherlands, Poland, and Slovakia.

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

Table of contents

INFORM project 3

List of Abbreviations 6

Chapter 1: Introduction 7

1.1 EU Directive (EU) 2016/680 7

1.2 Scope of EU Directive (EU) 2016/680 and delimitation from GPDR 8

1.3 Aims of this report 13

Chapter 2: Subject matter and terminology 14

Chapter 3: Principles for data processing 18

3.1 Main principles 18

3.2 Time limits and storage of data 19

3.3 Lawfulness of processing and specific processing conditions 22

3.4 Special categories of data 23

3.5 Profiling and automated decision making 24

Chapter 4: Data subject and data subject rights 26

4.1 Limitations and exercise of data subject rights 26

4.2 Information to be made available to the data subject 29

4.3 Direct access as a general rule 32

4.4 Right to rectification or erasure and restriction of processing 33

4.5 Indirect access to rights of data subject 37

Chapter 5: Remedies, liability and penalties - DPA 38

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

Chapter 6: Conclusions 41

Bibliography.....43

Case law 44

Appendix A: State of Directive (EU) 2016/680 transposition in Member States – December 2017 45

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

List of Abbreviations

1) **Directive (EU) 2016/680** - Directive (EU) 2016/680 of the European Parliament and of the Council of 27th of April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA;
2) **Framework Decision 2008/977/JHA** - Council framework decision 2008/977/JHA on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters;
3) **GDPR** - Regulation (EU) 2016/679 of the European Parliament and of the Council of 27th of April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation);
4) **Directive 95/46/EC** - Directive 95/46/EC of the European Parliament and of the Council of 24th of October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;
5) **DPAs** - Data Protection Authorities.

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

Chapter 1: Introduction

1.1 Directive (EU) 2016/680

Directive (EU) 2016/680 of the European Parliament and of the Council of 27th of April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (further referred to as Directive (EU) 2016/680) is the most recent legislation of the EU for the specific protection of personal data in the prevention, investigation, detection/prosecution of criminal offences and enforcement of criminal penalties. This piece of legislation which came into force on the 5th of May 2016 repealed the Council framework decision 2008/977/JHA on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters (further referred to as Framework Decision 2008/977/JHA).

A brief analysis of both legislations titles will reveal that Directive (EU) 2016/680 is a broader legal act which intends to be more encompassing than repealed Framework Decision 2008/977/JHA. Recital 5 of the Directive (EU) 2016/680 states that the Framework Decision 2008/977/JHA applies in the areas of judicial cooperation in criminal matters and police cooperation. The scope of application of that Framework Decision being limited to the processing of personal data transmitted or made available between Member States. Therefore Directive (EU) 2016/680 aims to ensure more consistent and higher level of protection of the personal data of natural persons in the areas of criminal matters and public security.

It is important to stress that Directive (EU) 2016/680 was adopted together with the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27th of April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (further referred to as GDPR) which indicates the attempt to ensure the integrity and complexity of data protection reform. The Directive (EU) 2016/680 ought to be considered as a *lex specialis* for personal data protection in criminal law whereas the GDPR is the *lex generalis* for personal data protection.

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

Directive (EU) 2016/680 requires EU Member States to achieve the result of a certain level of personal data protection in the field of criminal law without dictating the means of achieving that result. Therefore, the Directive (EU) 2016/680 binds Member States which are obliged to adopt certain principles in their legal systems. On the other hand, the GDPR is an EU regulation which applies directly to all EU citizens, companies and government organisations. The GDPR is mostly self-executing and does require limited implementing measures. Nevertheless, most of the European Member States now take steps to ensure proper application of the GDPR and therefore change its laws accordingly. The European legislator stipulated that both GDPR and Directive (EU) 2016/680 will become effective as of May 2018. Therefore, according to Article 63 of the Directive, the deadline for the implementation of the Directive into national laws ends on the 6th of May 2018, although many of the Member States may not be able to meet this deadline[1].

Directive (EU) 2016/680 regulates the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties[2]. Thus, Directive (EU) 2016/680 regulates personal data processing carried out by entities involved in the criminal justice system framework, such as the police authorities, public prosecutors, courts and the prison system within their legal tasks such as preventing, investigating, prosecuting and sentencing crimes, as well as executing criminal penalties. Any other processing activity, (outside the Directive (EU) 2016/680 scope) will be covered by GDPR (*lex generalis* regarding personal data processing).

1.2 Scope of EU Directive (EU) 2016/680 and delimitation from GPDR

The GPDR is well and widely recognized by various stakeholders' legal act, from European citizens (data subjects) to companies (smaller and bigger ones) as well as governmental institutions. The cause of such "popularity" is the big change in the data protection framework on the one hand and on the other hand - the possibility to impose significant administrative fines in the case of non-compliance by data protection supervisory authorities. These fines can be as high as 10 or 20 million euros (depending

[1] For more specific information please see Appendix 1.
[2] Subject-matter and objectives of Directive (EU) 2016/680 laid in art. 1 par. 1.

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

on the violation) or, in the case of an undertaking, up to 2 or 4 % of the total worldwide annual turnover of the preceding financial year, whichever amount is higher.

Directive (EU) 2016/680 on the processing of personal data in criminal law is much less known. Processing of personal data by competent authorities (e.g., the police, public prosecution services, courts and the prison system) for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties narrows the scope of Directive (EU) 2016/680.

In order to have a clear insight into the reviewed legal act it is important to undertake a delimitation between the Directive (EU) 2016/680 and the GDPR. The delimitation shall rely on the EU law notion of a criminal offence in view of establishing a harmonised scope of application of the Directive (EU) 2016/680. It should be noted that a delimitation based only on the text of those two legal acts (GDPR and Directive (EU) 2016/680) is virtually impossible. Given the various legal systems in EU Member States such a delimitation should be based upon complex information deriving from a comprehensive analysis of the Member States legal systems.

In regard to subjective (material) scope of Directive (EU) 2016/680 the delimitation between the GDPR and the Directive is quite difficult. However, the division line between administrative and criminal law should be clear for those who want to apply appropriate data protection provisions. While administrative law would fall under the GDPR, criminal law would be covered by the Directive (EU) 2016/680. Recital 13 states that a criminal offence within the meaning of Directive (EU) 2016/680 should be an autonomous concept of European Union law as interpreted by the Court of Justice of the European Union (CJEU). In other words, Member States cannot determine the nature of an offence as being "criminal" for the sole purpose of applying the Directive (EU) 2016/680. Instead, Member States should rely on what in the national legal order is already formally defined as a criminal offence.

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

Directive (EU) 2016/680 covers the processing activities of police and law enforcement authorities related to threats that may lead to a criminal offence. Criminal court proceedings are also covered by the Directive (EU) 2016/680.

Examples of data processing which fall within Directive (EU) 2016/680:

1. Processing the personal data of a suspect by the law enforcement authority in regard to ongoing investigation.
2. Processing the personal data of a defendant by the court in regard to ongoing criminal proceedings.

On the other hand, processing human resources data of law enforcement authorities, asylum or border control is not covered by the Directive (EU) 2016/680 and falls under the GDPR.

Examples of data processing which falls within GDPR:

1. Processing the personal data of employee by the law enforcement authority in order to pay social security.
2. Processing the personal data of asylum seeker by the public authority in regard to asylum proceedings (e.g. assessment of asylum application).

The personal scope of Directive (EU) 2016/680 includes competent public authorities but also private entities exercising public powers that are inherent of law enforcement authorities, such as judicial and police powers including the power to arrest[3]. All data controllers under the Directive (EU) 2016/680 must be competent authorities, but a competent authority can be organised in a way to encompass

[3] Minutes from the third meeting of the Commission expert group on the Regulation (EU) 2016/679 and Directive (EU) 2016/680, 7th of 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 deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

more than one data controllers within its structure[4]. For example, in case if a competent authority has various branches in various cities of a Member State and every branch undertakes various data processing activities, every and each branch may be data controller.

Public-Private Partnerships (PPPs) under Directive (EU) 2016/680 can only qualify as data controllers if they process data for the purposes of the Directive (EU) 2016/680, they decide on the purposes and means of the data processing and have been entrusted, by law, with public authority and public powers. In other cases, PPPs qualify as processors either:

1. under the Directive, where processing is done on behalf of competent authorities for the purposes of the Directive, or
2. under the GDPR where the processing is carried out for other purposes[5].

It should be also pointed out, that in regard to some Member States an issue of specific regulated professions occurs. Some authorities are able to carry out investigations or even prosecute a criminal offence e.g. financial intelligence units set up under the Directive (EU) 2015/849 of the European Parliament and of the Council of 20th of May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC. Such financial intelligence units in some Member States are administrative authorities, while in others they are considered as law enforcement authorities. During the transposition of Directive (EU) 2016/680 proceedings Member States shall distinguish between the administrative offences (covered by the GDPR) and criminal offences (covered by the Directive (EU) 2016/680).

In short, a competent authority, as defined in Directive (EU) 2016/680, means any (in principle public) entity acting, even if sporadically, to prevent, investigate, detect or prosecute of criminal offences or

[4] Minutes from the ninth meeting of the Commission expert group on the Regulation (EU) 2016/679 and Directive (EU) 2016/680, 4th of May 2017.
[5] *Ibidem*.

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

to execute criminal penalties and needs to process personal data strictly to that end. It should be highlighted that personal scope of the Directive (EU) 2016/680 is immanently bound with material scope of it.

It is important to emphasise that data subject's consent is not intended to provide a legal basis for processing personal data by competent authorities under Directive (EU) 2016/680. Of course, this is a consequence of the very limited degree of transparency for data processing determined by the Directive due to its aim of ensuring an effective prevention, investigation, detection or prosecution of criminal offences and execution of criminal penalties[6].

It should be highlighted that Directive (EU) 2016/680 regulates personal data processing carried out by entities involved in the criminal justice system framework, such as the police authorities, public prosecutors, courts and the prison system within their legal tasks such as preventing, investigating, prosecuting and sentencing crimes, as well as executing criminal penalties.

Any other processing activity, (outside the Directive (EU) 2016/680 scope) will be covered by GDPR (*lex generalis* regarding personal data processing).

Summary:

1. Directive (EU) 2016/680 sets rules for the processing in personal data in regard to criminal law matters (prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties).
2. Engel criteria shall be applied in order to define criminal offence (subjective scope of Directive (EU) 2016/680).
3. Directive (EU) 2016/680 is *lex specialis* in regard to processing of personal data whereas GDPR is *lex generalis*.
4. Not every law enforcement authority activity will be covered by Directive (EU) 2016/680, some of those activities will be covered by GDPR (employment issues, etc.).

[6] See also "Chapter 3: Principles of data processing".

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

5. Directive (EU) 2016/680 will be applicable only when both the material and the personal scope are present.
6. The data subject's consent does not provide a legal basis for processing personal data by competent authorities under Directive (EU) 2016/680.

1.3 Aims of this report

The INFORM project (INtroduction of the data protection reFORM to the judicial system) is a project that contributes to the further promotion, implementation and application of the GDPR and Directive (EU) 2016/680, with a specific focus on the judiciary, legal practitioners and court staff. The aim of the INFORM project is to provide judicial training for trainers from all EU Member States. INFORM project targets three distinguished groups within the judicial system: the judiciary (including judges and public prosecutors), legal practitioners (including lawyers, notaries, bailiffs) and court staff. This document (D2.5) reviews Directive (EU) 2016/680 for the legal practitioners.

This review involves a general description of Directive (EU) 2016/680, delimitation between GDPR and Directive (EU) 2016/680 as well as a short explanation and elaboration of the Directive in regard to legal practitioners. It should be stressed that generally the provisions in Directive (EU) 2016/680 are not aimed at the legal practitioners at all, but to entities involved in the criminal law proceedings (police officers, prosecutors) and their activities - prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties. Therefore, this report is rather a general review of chosen parts of Directive (EU) 2016/680 and tries to analyse them from legal practitioners' point of view to explain the (marginal) impact it may have on practicing law in the European Union.

As a consequence, the scope of this review mainly focuses on the data subject rights under Directive (EU) 2016/680 since they are persons of interest (potential clients) to legal practitioners (lawyers, legal advisers, attorney-at-laws, etc.), Therefore, further explanation is provided to clarify the meaning of the Directive in view to the rights of data subjects in order to provide a better understanding of this act for the legal practitioners. As a primary outcome, the overall awareness of legal practitioners for 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 deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

more effective protection of natural persons' rights regarding the processing of personal data should increase as a result of this report and its respective promotion.

For a review of the GDPR aimed at the legal practitioners, see Deliverable 2.4, created under the framework of the INFORM project.

In addition, this report shall become the basis of the training materials that are to be elaborated under the scope of the INFORM project. More information on the training materials, workshops, e-learning programs and INFORM days could be found on INFORM website: http://informproject.eu/

Chapter 2: Subject matter and terminology

Data protection in general is the protection of information regarding natural persons, which information could serve identify a natural person by reference to some factors such as name, identification number, location data etc.

As stated above, Directive (EU) 2016/680 is *lex specialis* in regard to data protection legislation and regulates in the field of criminal law chain. Nevertheless, it is important to stress that basic terminology is virtually the same as in *lex generalis* (GDPR). Therefore, the definition of personal data in the Directive is identical to the one in Art. 4 No. 1 of the GDPR.

„Personal data" is defined in Art. 3 No. 1 of Directive (EU) 2016/680 as "any information relating to an identified or identifiable natural person („**data subject**"). It goes further to define "an **identifiable natural person** as 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"[7]. The CJEU has characterised personal data by referring to a person's name,

[7] See art. 3 par. 1 of Directive (EU) 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 deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

telephone number and information about his working conditions[8] and also fingerprints as they can be used to identify individuals with precision[9], and IP address if the data allows to identify person[10].

The definition explicitly encompasses „location data and an online identifier" of natural persons which clarifies the material scope in comparison to the former Framework Decision 2008/977/JHA. Directive (EU) 2016/680 is therefore technology compliant in accordance with global technological advancements.

The abovementioned definitions clarify that data protection only applies to natural and identifiable persons. Legal persons (companies, foundations and other legal entities) are not protected by Directive (EU) 2016/680 (nor GDPR). Also, the personal data of deceased people does not fall within the scope of Directive (EU) 2016/680. It should be also noted that personal data processed with regard to criminal law is within the scope of Directive (EU) 2016/680, regardless of nationality or residence of data subjects.

Article 2 of Directive (EU) 2016/680 provides that the Directive applies to the processing of data by competent authorities. This provision differs from the analogous provision encompassed by Article 1 of the Framework Decision 2008/977/JHA and therefore the Directive (EU) 2016/680 is not limited to processing of personal data in the framework of police and judicial cooperation in criminal matters, provided for by Title VI of the Treaty on European Union but to all forms of processing falling within the objective of the said Directive. It does not apply to the processing of personal data by EU institutions, bodies, offices and agencies[11], therefore processing of personal data by the Europol[12] is outside the scope of the Directive (EU) 2016/680. Despite excluding Europol from its scope, Directive (EU) 2016/680 impacts directly on Regulation (EU) 2016/794 of the European Parliament

[8] C-101/01 Lindquist.
[9] C-291/12 Schwarz v. Bochum.
[10] C-582/14 Breyer v. Germany.
[11] See art. 2 par. 3 letter b of Directive (EU) 2016/680.
[12] Data protection principles binding Europol are put out in Chapter VI of Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA.

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

and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA (further referred to as Europol Regulation). Recital 40 of Europol Regulation highlights the importance of aligning this law with the Directive (EU) 2016/680: "(…) the data protection rules of Europol should be autonomous while at the same time consistent with other relevant data protection instruments applicable in the area of police cooperation in the Union. Those instruments include, in particular, Directive (EU) 2016/680 of the European Parliament and of the Council (12), as well as the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of the Council of Europe and its Recommendation No R(87) 15 (13)".

Directive (EU) 2016/680 regulates the data protection standards applicable within the Member States, which are the main sources of Europol's information[13], therefore interacts with Europol and Europol Regulation despite excluding Europol from its scope.

The scope of Directive (EU) 2016/680 is limited to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties including the safeguarding against and the prevention threats to public security[14]. The scope of this legal act also encompasses the processing of personal data completely or partially by automated means and other than by automated means that that is or will be part of a filing system (such as personal data in hardcopy case files)[15].

Example of personal data processing other than by automated means:

Personal data printed on paper stored on shelves in case files.

[13] M. O'Neill, K. Swinton (2017) Challenges and Critiques of the EU Internal Security Strategy. Rights, Power and Security, p. 162.
[14] See art. 1 and 2 of Directive (EU) 2016/680
[15] See art. 2 of Directive (EU) 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 deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

Article 1 par. 3 of Directive (EU) 2016/680 provides that Member States may provide for higher level of safeguards than those provided for in the Directive for the protection of the rights and freedoms of data subjects with regard to the processing of personal data by competent authorities. That provision shows the intention of the EU legislator to ensure that high level standards are applied for the purpose of data protection to ensure protection of the right to personal data protection.

The processing of personal data includes the 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 of personal data[16].

Example of personal data processing:

1) Collecting personal information of natural persons during an investigation.
2) Recording the testimony of a witness in criminal proceedings.
3) Organising and structuring the police archive of case files.
4) Storing case files by the prosecutor.
5) Adapting personal data on electronic form by a police officer.
6) Disclosing personal data of one law enforcement agency to another during criminal proceedings.
7) Destroying case files after the legal retention period is expired.

Recital 20, Recital 107 and Article 18 of the Directive (EU) 2016/680 explicitly mention that the Directive does not preclude Member States from specifying processing operations and processing procedures in national rules on criminal procedures in relation to the processing of personal data by courts and other judicial authorities, in particular regarding personal data encompassed in a judicial decision or in records in relation to criminal proceedings. It should be therefore noted that some types

[16] See art. 3 par. 2. of Directive (EU) 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 deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

of data processing, such as anonymization, transforms personal data into non-personal data, putting it beyond the reach of the data protection law.

Chapter 3: Principles for data processing

3.1 Main principles

Directive (EU) 2016/680 mainly repeats the principles of the data protection law established in Directive 95/46/EC.

Most of the principles of Directive (EU) 2016/680 are common to the ones outlined by GDPR and should therefore be interpreted in a consistent manner with it. Nevertheless, certain differences do exist. For example, the principle of transparency does not exist in the Directive (EU) 2016/680, although the principle of fair processing implies some degree of transparency[17]. Full transparency principle would interfere with ongoing criminal investigations. The principle of data minimisation is also different and offers more flexibility to the controllers under Directive (EU) 2016/680.

The processing of personal data must be lawful, fair and transparent and used for specific purposes mentioned in the pertinent law. The purpose of the processing should be explicit and legitimate, and determined when that data is collected. Individuals should be informed of the possible risks, rules, safeguards, and rights in relation to the processing of their personal data and how to use their rights[18].

Main principles for data processing:

- Lawfulness and fairness (art. 4 par. 1 letter a)
- Purpose specification and limitation (art. 4 par. 1 letter b)
- Data minimisation (art. 4 par. 1 letter c)

[17] Minutes of the third meeting of the Commission expert group on the Regulation (EU) 2016/679 and Directive (EU) 2016/680, 7th of November 2016.
[18] See recital 26 of Directive (EU) 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 deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

- Accuracy (art. 4 par. 1 letter d)
- Storage limitation (art. 4 par. 1 letter e)
- Appropriate security (art. 4 par. 1 letter f)
- Accountability (art. 4 par. 4)

Unlike the GDPR, Directive (EU) 2016/680 does not encompass the concept of further processing. Subsequent processing by the same or a different competent authority is allowed for other purposes of the Directive (EU) 2016/680, but such subsequent processing for purposes other than that the data were originally collected for, must meet the applicable legal requirements for the processing of personal data should be:

1) provided by law,
2) necessary, and
3) proportionate to the legitimate aim pursued[19].

The personal data collected and retained for purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties should not be kept and processed for unspecified or general purposes or in a way which would not comply with the principle of purpose limitation.

3.2 Time limits and storage of data

Article 5 of Directive (EU) 2016/680 states that Member States shall provide for appropriate time limits to be established for the erasure of personal data or for a periodic review of the need for the storage of personal data. In other words, the stored personal data must be reviewed and erased periodically after appropriate time limits.

[19] Minutes of the third meeting of the Commission expert group on the Regulation (EU) 2016/679 and Directive (EU) 2016/680, 7th of November 2016.

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

The concept of purpose/storage limitation is an important principle. It has two main aspects: data should only be used for limited purposes and it should only be retained for a limited amount of time[20].

Article 29 Working Party (further referred to as WP29) considers the possibility of mixed system allowing the combination of general maximum time limits with the periodical review of the need to keep for a further period the data stored in a way that allow the identification or the identifiability of the concerned data subject[21]. According to the opinion of WP29 this is the best way to ensure full compliance with the principles relating to processing of personal data laid down in Article 4 of the Directive (EU) 2016/680[22].

The personal data should be stored in different categories (e.g. victims, experts, suspects etc.), as provided in Article 6 of the Directive (EU) 2016/680, and automatically deleted after a given period, unless a periodic review reveals the need for prolonging the data retention period[23].

Example:

Information collected directly from a person's statement will be assessed differently than information collected from a person's hearsay statement.

Data based on facts, or 'hard' data, will be assessed differently than data based on opinions or personal assessments, or 'soft' data.

[20] Pajunoja, L.J. (2017) The Data Protection Directive on Police Matters 2016/680 protects privacy - The evolution of EU´s data protection law and its compatibility with the right to privacy, Master Thesis, Helsinki: University of Helsinki, p. 58; Bräutigam, T. The land of confusion: international data transfers between Schrems and the GDPR. T. Bräutigam & S. Miettinen, Data protection, privacy and European regulation in the digital age, p. 143-177.

[21] Article 29 Data Protection Working Party Opinion on some key issues of the Law Enforcement Directive (EU 2016/680) Adopted on 29 November 2017, p. 3.

[22] *Ibidem*.

[23] Minutes of the ninth meeting of the Commission expert group on the Regulation (EU) 2016/679 and Directive (EU) 2016/680, 4th of May 2017.

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

In this perspective, in principle, personal data should be processed until it serves the purpose for which it was collected and when it is no longer necessary for that purpose, it should be deleted, unless subsequent processing is foreseen by law and is deemed relevant for a purpose which is not incompatible with the original purpose for processing[24].

WP29 stressed out that national law should provide for clear and transparent criteria for the assessment of the necessity to further keep personal data, as well as for procedural requirements, so that the data quality principles are effectively met in order to avoid any abuse. Moreover, WP29 highlights that whenever such a periodic review is carried out, the WP29 supports the involvement of a data protection officer (DPO) in the application of such criteria - inter alia with a view to a possible internal audit - and information on any decision to further retain the data and the reasons behind it, should be kept and made available to the relevant supervisory authority[25].

Moreover, appropriate time limits should be established in accordance with the proportionality principle, therefore any decision to prolong the retention period should be supported by sufficient and valid reasons[26]. It is important to stress that GDPR does not mention time limits directly, but data retention and time limits of data processing may be deduced from storage limitation principle[27].

Example:

Time limit is set at 25 years after the release of convict from jail.

After that time, personal data of data subject regarding the criminal proceedings should be erased.

Article 6 of the Directive (EU) 2016/680 provides for a distinction between different categories of data subjects. The provision stipulates that a distinction shall be made between data belonging to suspects, convicts, victims and other parties relevant to the crime like witnesses. The Working Party

[24] Article 29 Data Protection Working Party Opinion on some key issues of the Law Enforcement Directive (EU 2016/680) Adopted on 29 November 2017, p. 4.
[25] *Ibidem,* p. 4.
[26] Minutes of the ninth meeting of the Commission expert group on the Regulation (EU) 2016/679 and Directive (EU) 2016/680, 4th of May 2017.
[27] See art. 5 par. 1 letter e) of GDPR.

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

on Police and Justice has recommended that the processing of personal data of non-suspects should be treated cautiously, and specific conditions and safeguards must be followed to avoid undue treatment of persons not involved in crime[28].

Facts based personal data must be separated from data which is based on personal assessments. The competent authorities should not make available nor transmit inaccurate and incomplete personal data and they should verify the quality of the data before processing[29]. When personal data is sent to other authority, the receiver should be able to evaluate its accuracy, completeness, and reliability. If incorrect personal data is transmitted or transmitted unlawfully, the recipient must be notified, and the data should be corrected or erased, or the processing restricted[30].

WP29 considers it to be a good practice, as well as a tool for monitoring compliance, that statistical information on the erasure of data and the review procedure is made available both to the DPO and to the DPA, if requested[31].

3.3 Lawfulness of processing and specific processing conditions

Article 8 of the Directive (EU) 2016/680 makes it mandatory to Member States to only permit processing of data when such is necessary for the performance of a task carried out by a competent authority for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties and that it is based on Union or Member State law.

Examples of lawful processing under Directive (EU) 2016/680:

1. Processing of data by competent authority for the purpose of the execution of criminal penalty.

[28] Working Party on Police and Justice; The Future of Privacy. Joint contribution to the consultation of the European Commission on the legal framework for the fundamental right to protection of personal data, adopted on 01 December 2009, page 26.
[29] Pajunoja, L.J. (2017) The Data Protection Directive on Police Matters 2016/680 protects privacy - The evolution of EU´s data protection law and its compatibility with the right to privacy, Master Thesis, Helsinki: University of Helsinki, p. 58.
[30] See art. 7 of Directive (EU) 2016/680.
[31] Article 29 Data Protection Working Party Opinion on some key issues of the Law Enforcement Directive (EU 2016/680) Adopted on 29 November 2017, p. 4.

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

2. Processing of data by police for the purpose of crime investigation.

Article 9 of the Directive (EU) 2016/680 sets out the specific conditions for the processing of data by a competent authority. Personal data collected by competent authorities for the purposes of Directive (EU) 2016/680 shall only be processed for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties unless such processing is authorized by Union or Member State law[32]. The collection of personal data for prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties purposes should be limited to what is necessary and proportionate for the prevention of crime risk or the prevention, investigation and prosecution of a specific criminal offence as well as execution of criminal penalties. Any exception to this provision should be the subject of specific national legislation. An evident and direct correlation should exist between the data processing carried out by the competent authority and a situation where individuals have already committed or are likely to commit a crime.

The competent authority should always choose an adequate legal basis to process personal data and should process personal data in a legitimate way. A careful assessment should be carried out by the competent authority to ensure that the processing is based on an appropriate legislation and the procedures for data processing foreseen by it are fully respected[33].

Where personal data is being processed for other purposes outside the scope of Directive (EU) 2016/680, GDPR shall apply unless the processing is carried out in an activity which falls outside the scope of the European Union law.

3.4 Special categories of data

Crucial provision is one limiting the processing of special categories of data with the notable inclusion of genetic data and biometric data capable of identifying a natural person which was not special categories of data under Art. 6 of the Framework Decision 2008/977/JHA. The rationale for the inclusion of genetic data as above may be the need to unify the protection of special data categories

[32] See art. 9 par. 1 of Directive (EU) 2016/680.
[33] D. Allen, E. van Beek, J. Borking (2018) Practical guide on the use of personal data in the police sector, p. 3.

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

under the GDPR and under the Directive (EU) 2016/680. Nevertheless, Article 10 of the Directive (EU) 2016/680 on special categories of personal data differs in approach from the corresponding Art. 9 of the GDPR. In the Directive, the legal basis for any processing must be found in law (according to Article 8 of the Directive (EU) 2016/680), and one of the three conditions (authorisation in law, protection of vital interests of the data subject or another natural person, data manifestly made public) must be met in order to process sensitive data, together with legal safeguards (where consent of the data subject is an example of an appropriate safeguard)[34] and must be strictly necessary.

Special categories of data:

1) race,
2) ethnic origin,
3) politics,
4) religion or philosophical beliefs,
5) trade union membership,
6) genetics,
7) biometrics (where used for ID purposes),
8) health,
9) sex life, or
10) sexual orientation.

3.5 Profiling and automated decision making

Profiling and automated decision making are more and more developed in many sectors, including in the area covered by Directive (EU) 2016/680. The Directive (EU) 2016/680 defines "profiling" in Article 3 par. 4 as 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

[34] Minutes of the fifth meeting of the Commission expert group on the Regulation (EU) 2016/679 and Directive (EU) 2016/680 from 18th of January 2017.

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

aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. Therefore Directive (EU) 2016/680 uses a wording coincident with the one used in the GDPR.

Solely automated decision-making refers to the ability to make decisions by technological means without human involvement in the decision process. Profiling and automated decision-making can be combined activities of the same process, they can also be carried out separately.

Example of automated individual decision making:

- Automatic decision regarding refusal of granting a better meal at prison canteen due to repeated misbehaviour recorded by CCTV footage and processed in IT system.

Article 11 of Directive (EU) 2016/680 establishes a general prohibition on solely automated individual decision, including profiling, having an adverse legal effect or significantly affecting the data subject. The only exception to this prohibition is that such automated decision is authorized by Union law or a Member State law that provide suitable safeguards for the rights and freedoms of data subjects. However, the same Article considers that such prohibition is valid also in respect of a decision "significantly affecting" the individual such as for example in the case where a passenger is not allowed on board because registered in a black list, thereby expanding the scope of Article 11 of Directive (EU) 2016/680[35].

Member States' national legislator, when authorizing the decision based solely on automated processing under Article 11, must provide data subjects with the right to obtain human intervention on behalf of the controller[36]. Although Article 11 only refers to the right to obtain human intervention, it should be noted that according to Recital 38 of the Directive, in any case, such processing should be subject to suitable safeguards, including the "right to obtain human intervention", in particular to

[35] Article 29 Data Protection Working Party Opinion on some key issues of the Law Enforcement Directive (EU 2016/680) Adopted on 29 November 2017, p. 12.
[36] See art. 11 par. 1 of Directive (EU) 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 deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

express his or her point of view, to obtain an explanation of the decision reached after such assessment or to challenge the decision"[37].

Human intervention here is a key element: it allows the data subject not to be submitted to indecipherable automated decisions which may suffer from errors or bias and allows him/her to have an exchange with the controller open to the additional elements or contestation the data subject may want to raise[38].

The creation of profiles based on special categories of data which may lead to discrimination is prohibited by Article 11 par. 3, in accordance with EU law. Discrimination is unquestionably an example of a decision that significantly affects the data subject and may entail adverse legal effects as well[39]. Therefore, Member States should consider that the national law transposing the Directive may not, under any circumstance, authorise profiling, that results in discrimination if based on the processing of sensitive data[40] whilst the automated decision making based on sensitive data is allowed, but only in the presence of a legal basis under EU or national law – which provides for the safeguards[41].

Chapter 4: Data subject and data subject rights

4.1 Limitations and exercise of data subject rights

Directive (EU) 2016/680 dedicates one chapter on data subject's rights, which are in the focus of this review. Above all, it should be made clear which information must be made available to the data subject in accordance with the data subject's right of access to personal data, the right to rectify or erase data

[37] Article 29 Data Protection Working Party Opinion on some key issues of the Law Enforcement Directive (EU 2016/680) Adopted on 29 November 2017, p. 12.
[38] Ibidem.
[39] Ibidem.
[40] See art. 11 par. 3 of Directive (EU) 2016/680.
[41] See Article 11 par. 1 and par. 2 of Directive (EU) 2016/680. Also, Directive (EU) 2016/681 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, art. 6 par. 4 and Recital 15. Article 29 Data Protection Working Party Opinion on some key issues of the Law Enforcement Directive (EU 2016/680) Adopted on 29 November 2017, p. 12.

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

or to restrict the processing, and rights in criminal proceedings. Data subjects should also be informed when his or her rights are limited and on what grounds. Moreover, it should be emphasised that the competent supervisory authority may exercise and verify the data subject's rights[42].

Data subject rights provided in Directive (EU) 2016/680 are similar to those provided in GDPR. For an overview please see the table below, which demonstrates that most of the rights have an identic title, though they are limited in comparison to the ones in the GDPR. In regard to Directive (EU) 2016/680, Member States may impose restrictions to avoid for example obstructing investigations or criminal procedures. A more complex review of the rights is provided below.

Data subject right	Directive (EU) 2016/680	GDPR
Right to information	Art. 12-14	Art. 12-13
Right to access	Art. 14-15	Art. 15
Right to rectification	Art. 16	Art. 16
Right to erasure (Right to be forgotten)	Art. 16	Art. 17
Right to restriction of processing	Art. 16*	Art. 18
Right to data portability	X	Art. 20
Right to object to automated individual decision-making	X	Art. 21-22

Table 1. Data subject rights under Directive (EU) 2016/680 and GDPR

[42] Art. 12 - 18 of Directive (EU) 2016/680 although Article 29 Working Party believe that art. 12 of Directive (EU) 2016/680 contains mere controller/processors obligation. For further information see Opinion WP 2017/258 on some key issues of the Law Enforcement Directive (EU 2016/680). Adopted 20 November 2017.

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

The limitations to the data subject's rights of access are set in Art. 15, which allows Member States to adopt measures which restrict the data subject's right of access the data, as long as such a restriction constitutes a necessary and proportionate measure for the reasons listed in Article 15 par. 1 of the Directive (EU) 2016/680.

Exemptions from the fundamental rights and legitimate interests of the natural person should be applied as an exception rather as the rule and that omitting information may be allowed within an investigation only for as long as such a restriction constitutes a necessary and proportionate measure[43].

The omitted information must, in accordance with the case law of the CJEU, be provided once it is no longer liable to jeopardize the investigations being carried out[44].

If the data subject's right of access has been only partially limited, the controller should provide access to the personal data being processed and the information listed in Article 14. A summary of the data in possession of the controller could be provided[45] (e.g. copy of data on a durable medium).

If the controller wishes to fully restrict the right of access, Member States shall provide that the controller must inform the data subject, without undue delay, in writing, confirming the refusal or restriction of access and the reasons. Moreover, controllers ought to document the factual or legal reasons for that decision and such information must be made available to the supervisory authorities upon request [46].

Member States should ensure that controllers always provide an answer to a right of access request and that in case the right of access is being restricted or denied, the data subject is provided with

[43] Opinion WP 2017/258 on some key issues of the Law Enforcement Directive (EU 2016/680). Adopted 20 November 2017.
[44] *Ibidem*, Opinion 1/15 of the European Union Court of Justice on the Draft PNR Agreement between Canada and the European Union, 26 July 2017; see also case Tele2 Sverige and Watson and Others judgment of European Union Court of Justice 21 December 2016.
[45] See recital 43 of Directive (EU) 2016/680.
[46] Opinion WP 2017/258 on some key issues of the Law Enforcement Directive (EU 2016/680). Adopted 20 November 2017.

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

information regarding the right to lodge a complaint with a supervisory authority and the contact details of this Data Protection Authority or the option to seek a judicial remedy[47].

Article 12 of Directive (EU) 2016/680 stipulates that Member States are to provide information to data subjects in „concise, intelligible and easily accessible form, using clear and plain language". The essence of this new provision is to ensure that all information provided to data subjects regarding the obligation deriving from Directive (EU) 2016/680 serves the purpose of actually informing such data subjects and ensuring transparency of processing, which ensures that the lawful processing of personal data is fair.

It should be emphasised that there is a difference between the direct and indirect exercise of data subject rights. The rule is direct exercise by the data subject, while indirect exercise comes into play when certain information about the imposed restrictions are not provided to the data subject, for duly justified reasons. It is important to note that the provisions on the rights of data subject, like the entire Directive (EU) 2016/680, are fully applicable in criminal proceedings[48].

4.2 Information to be made available to the data subject

Article 13 states the information to be provided to the data subject without distinguishing whether the information is obtained from the data subject or not as stipulated in Directive 95/46/EC and creating the obligation to provide more information by data controller. This ensures that uniform rules apply to all data subjects with exceptions to the protection of rights which ought to "overwrite" the right to data protection such as protection of life, prosecuting of crime, etc.

Processing data under the scope of the Directive (EU) 2016/680 may sometimes be used in a manner that could cause some detriment to an individual. This is important as the processing of data under the Directive results in limitations on the individuals' freedoms and rights and is performed, at times, without the individuals being aware[49] of the processing.

---

[47] Ibidem.
[48] Minutes of the fifth meeting of the Commission expert group on the Regulation (EU) 2016/679 and Directive (EU) 2016/680 from 18th of January 2017.
[49] Opinion WP 2017/258 on some key issues of the Law Enforcement Directive (EU 2016/680). Adopted 20 November 2017.

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

Article 13 par. 1 lit. a to e is about general information to be provided to the public and defines the information the controller has to make available to data subjects. It should be noted that the wording of Article 13 par. 1 refers to „making available" information.

Information which should be made available to the data subject (Art. 13 par. 1):

1) identity of the controller,
2) existence of the processing operation,
3) purposes of the processing,
4) right to lodge a complaint,
5) existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing[50]

Examples of making available:

1) website, where police force publishes their privacy policy in relation to the use of custody images;
2) easy accessible board in controller's main building, where police publish their privacy policy in relation to firearms registration;
3) website, where police force publishes their privacy policy in relation to the use of Body Worn Video[51].

Article 13 par. 2 uses „giving" information „in specific cases"[52]. This points to a difference in approach, whereby it can be argued that this obligation does not relate to a certain data subject, but to a certain

[50] See art. 13 par. 1 of Directive (EU) 2016/680.
[51] Opinion WP 2017/258 on some key issues of the Law Enforcement Directive (EU 2016/680). Adopted 20 November 2017.
[52] *Ibidem*.

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

processing procedure and all data subjects potentially affected by it, which implies that the information must be effectively made available in order to ensure that any data subject possibly concerned has been notified of them[53]. In other words, information which should be given in accordance to Article 13 par. 2 should be targeted to the affected data subject, not to the general public.

Information which should be given to the data subject in specific cases (art. 13 par. 2):

1) the legal basis for the processing;
2) the period for which the personal data will be stored, or, where that is not possible, the criteria used to determine that period;
3) where applicable, the categories of recipients of the personal data, including in third countries or international organisations;
4) where necessary, further information, in particular where the personal data are collected without the knowledge of the data subject.[54]

Examples of giving information:

1) data is collected directly from the data subject, e.g. hearing of witness during investigation;
2) indirectly without the knowledge of the data subject, e.g. net tracking, smart surveillance, etc.

Member States may adopt legislative measures delaying, restricting or omitting the provision of the information listed in Article 13 par. 2 to the data subject to the extent that it is necessary and proportionate in order to avoid any of the prejudices outlined in Article 13 par. 3. Any legislative measures must have due regard to the fundamental rights and the legitimate interests of the data

[53] *Ibidem*.
[54] See art. 13 par. 2 of Directive (EU) 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 deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

subject[55]. Articles 13 par. 4 and 15 par. 2 do not allow for blanket restrictions to data subject rights to information and access[56].

4.3 Direct access as a general rule

Article 14 of Directive (EU) 2016/680 entitles the data subject to the right to be informed what information pertaining to him/ her is being processed as well as the right to access to personal data being processed from the controller. Information should be provided free of charge without undue delay[57]. This right is subject to conditions and limitations similar to those in the mentioned Article 13 of Directive (EU) 2016/680. Article 14 provides for in the right of access of the data subject to their personal data. This provision derives from Article 12 lit. a of Directive 95/46/EC, with the addition of new elements for information of the data subjects such as the storage period, their rights to rectification, erasure, or restriction and to lodge a complaint.

Type of information under right of access (art. 14):

1) the purposes of and legal basis for the processing;
2) the categories of personal data concerned;
3) the recipients or categories of recipients to whom the personal data have been disclosed, in particular recipients in third countries or international organisations;
4) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
5) the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject;

[55] Opinion WP 2017/258 on some key issues of the Law Enforcement Directive (EU 2016/680). Adopted 20 November 2017.
[56] *Ibidem*.
[57] WP29 is of the view that controllers should provide information in response to a request under Article 14 to the data subject as soon as possible, where feasible within one month, for further information see Opinion WP 2017/258 on some key issues of the Law Enforcement Directive (EU 2016/680). Adopted 20 November 2017.

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

6) the right to lodge a complaint with the supervisory authority and the contact details of the supervisory authority;

7) communication of the personal data undergoing processing and of any available information as to their origin (all relevant information on how and under which circumstances the controller received them).

Example of exercising the right of access:

John Doe, a witness of a crime occurred in June 2018, being heard during investigation, wants to know whether his data is still processed in 2020 (case closed in December 2018). In order to receive information, he contacts the Data Protection Officer in the respective Police Force which had the jurisdiction over the case. The DPO, as the contact point, provides the information regarding John Doe.

4.4 Right to rectification or erasure and restriction of processing

Article 16 of Directive (EU) 2016/680 contains a more complex provision for the right to be forgotten/rectification/restriction of processing as opposed to that provided for in Article 16-18 of the GDPR.

The measures in art. 16 of Directive (EU) 2016/680 provide a framework on the processing activities that covers accurate data, which is of utmost importance for effective and just prevention, investigation, detection/prosecution of criminal offences and enforcement of criminal penalties on the one hand and privacy of data subject, on the other. Processing of inaccurate data may have adverse effects on the data subject, therefore data should be rectified in particular where it relates to facts[58], and the data subject has requested rectification. Controllers have also the obligation to erase personal

[58] See recital 47 of Directive (EU) 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 deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

data and to enable the right of data subjects to obtain the erasure of personal data concerning them from the controller when the processing infringes the Directive (EU) 2016/680[59].

The data subject has a right to erase his or her data when this data is incorrect, processed unlawfully or violates the requirements for processing data which fall under special categories of data[60]. Data subjects have the right to rectify inaccurate personal data relating to them, in particular when it relates to facts, as well as, taking into account the purposes of the processing, the right to have incomplete data completed, including by means of providing a supplementary statement[61].

The erasure of personal data is required where it was obtained from processing which infringes the principles relating to the processing of personal data, where it is unlawful, infringes the provisions of the Directive 680/2016 on the processing of special categories of personal data, or where personal data must be erased to comply with a legal obligation to which the controller is subject[62]. The WP29 states that if following a request to erase personal data, controllers determine that the personal data must be maintained for the purpose of evidence and where the accuracy of the personal data is contested by the data subject and the accuracy of that data cannot be determined, the Directive (EU) 2016/680 foresees the right to obtain the restriction of processing instead of erasure from the controller[63].

Directive (EU) 2016/680 does not *expressis verbis* foresee the right to restriction separate from the right to erasure as it is enshrined in Article 18 of the GDPR. Nevertheless, recitals 47 and 48 of the Directive (EU) 2016/680 mention this right distinctly, therefore, the WP29 stated that Member States should consider the creation of such a right for data subjects in their national legislation, both as a corollary to the right of erasure and as a distinct right for the data subjects who should be able to ask for the

[59] See art. 16 par. 2 and recital 47 of Directive (EU) 2016/680
[60] See article 16 of Directive (EU) 2016/680.
[61] See recital 47 of Directive (EU) 2016/680; Opinion WP 2017/258 on some key issues of the Law Enforcement Directive (EU 2016/680). Adopted 20 November 2017.
[62] Opinion WP 2017/258 on some key issues of the Law Enforcement Directive (EU 2016/680). Adopted 20 November 2017.
[63] Ibidem. WP29 recommended that such restrictions should be documented and mention for instance when the limitation started and stopped, furthermore in case of a restriction of the processing the data should also not be sent to other controllers until the restriction is lifted.

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

restriction of processing in other cases than the two situations foreseen in paragraph 3 of Article 16, especially in cases where erasure will have been refused by the controller without restricting the processing[64].

Article 16 par. 4 of Directive (EU) 2016/680 provides the option for Member States to restrict, either fully or partially, the written information to be provided to the data subject concerning the refusal by the controller to rectify or erase the data, or to restrict the processing and the reasons for this refusal. If the controller refuses the request for erasure or rectification, the controller will have to provide written information regarding the refusal as well as the reasons for the refusal.

It is very important to stress that although the Directive only foresees the possibility to restrict the provision of this information to the data subject in case of refusal by the controller, WP29 underlined that it should be clear that in cases where it is established that the data is inaccurate or incomplete, or that data is processed in violation with Articles 4, 8 or 10 Directive (EU) 2016/680, the controller shall not be able to refuse the rectification or erasure of the data[65].

Grounds for Member States to restrict right to rectify or erase the data (art. 16 par. 4):

1) avoid obstructing official or legal inquiries, investigations or procedures;
2) avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties;
3) protect public security;
4) protect national security;
5) protect the rights and freedoms of others[66].

[64] *Ibidem.*
[65] *Ibidem.* Moreover Article 29 Working Party recommended that Member States should provide for the categories of processing and situations where the controllers will never be allowed to, wholly or partly, refuse to rectify or erase the data or restrict the processing.
[66] See art. 16 par. 4 of Directive (EU) 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 deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

Controllers should provide an answer to a right to erasure or rectification request and if the right is being restricted or denied, that the data subject is provided with information regarding the right to lodge a complaint with a supervisory authority or the option of seeking a judicial remedy[67].

Any exemptions from the fundamental rights and legitimate interests of the natural person should not be applied as the rule and interpreted in a restrictive manner, as regularly recalled by the ECHR including the limitations of the rights of data subjects[68].

The controller must ensure that the rectification of the data concerned is communicated to the original controller who collected the personal data and any recipients of that data. Those recipients must also similarly rectify, erase or restrict the processing of the personal data concerned.

Example of exercising the right to rectify or erasure of personal data and restriction of processing:

1) Rectification

Jane Doe, a witness of a crime occurred in June 2018, being heard during investigation by the Police Force in August 2018. The criminal court started the criminal proceedings in April 2019. Jane Doe changed her name to Jones and her address as well as she had recently wed. She informed the Police Force that she changed name and address. The Police Force then informed the competent criminal court in this matter.

2) Erasure

James Franco, a suspect of a crime which occurred in September 2018, was found innocent of all charges in January 2019. After 5 years, he filed for erasure of part of his personal data (special categories), which was collected unlawfully, and the criminal court confirmed the unlawful collection of data during criminal proceedings.

[67] Opinion WP 2017/258 on some key issues of the Law Enforcement Directive (EU 2016/680). Adopted 20 November 2017.
[68] Cases S. and Marper v. UK, ECHR, 2008, or M.K v. France, ECHR, 2013

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

4.5 Indirect access to rights of data subject

Data subject have the right to exercise his/ her rights through the competent supervisory (indirectly). Such indirect access to rights of data subject is possible when:

a) the data subject rights to information, access, or information about refusal of rectification or erasure have been restricted by the controller,
b) on the basis of legislative measures allowing for restrictions, and
c) the abovementioned rights could not have been exercised directly to the controller[69].

Indirect exercise comes into play only when certain information about the imposed restrictions are not provided to the data subject, for duly justified reasons[70]. The option to have data subject's rights exercised through the competent authority has to be seen as an additional guarantee offered to the data subjects in the context of Directive (EU) 2016/680. GDPR does not foresee such a possibility when rights of data subjects will have been restricted.

Controllers must inform data subjects of the possibility to exercise their rights through the supervisory authority[71].

Information of controller in regard to indirect access should be:

1) clear,
2) intelligible,
3) given as soon as possible by the controller to the data subject, and
4) include the contact details of the competent supervisory authority[72].

[69] Opinion WP 2017/258 on some key issues of the Law Enforcement Directive (EU 2016/680). Adopted 20 November 2017.
[70] Minutes of the fifth meeting of the Commission expert group on the Regulation (EU) 2016/679 and Directive (EU) 2016/680 from 18th of January 2017.
[71] See art. 17 par. 2 of Directive (EU) 2016/680.
[72] Opinion WP 2017/258 on some key issues of the Law Enforcement Directive (EU 2016/680). Adopted 20 November 2017.

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

Competent supervisory authorities exercising "indirect access" rights must at least inform the data subject that all necessary verifications or a review have taken place and that he or she has the right to seek a judicial remedy[73].

Chapter 5: Remedies, liability and penalties - DPA

On the grounds of Directive (EU) 2016/680, as well as the GDPR, each Member State shall establish an independent supervisory authority (Data Protection Authorities, further referred to as DPA) which will be responsible for monitoring the application of Directive (EU) 2016/680[74]. Article 50 of Directive (EU) 2016/680 provides for mutual assistance among the DPAs of the Member States. This is a revolution of the provisions of Framework Decision 2008/977/JHA which did not provide any measures that could be compared to Article 50 of Directive (EU) 2016/680 in this regard.

Directive (EU) 2016/680 gives data subjects the right to lodge a complaint at a supervisory authority and a right to be informed about the progress, as well as the outcome of the complaint[75]. Data subjects are to be provided with a right to judicial remedy against the controller or processor[76].

Directive (EU) 2016/680 further outlines that DPAs shall have effective powers for investigations (Article 47 par. 1 of Directive (EU) 2016/680), effective corrective powers (Article 47 par. 2 of Directive (EU) 2016/680) and effective advisory powers (Article 47 par. 3 of Directive (EU) 2016/680) as well as the power to bring infringements of provisions adopted pursuant to the Directive to the attention of judicial authorities and, where appropriate, to commence or otherwise engage in legal proceedings, in order to enforce the provisions adopted pursuant to the Directive[77].

With regard to the corrective powers, Article 47 par. 2 of Directive (EU) 2016/680 only provides examples of what these powers could be, like the power to order the erasure or rectification of data or

[73] *Ibidem*.
[74] See Article 41 and 42 of Directive (EU) 2016/680.
[75] See Article 52 of Directive (EU) 2016/680.
[76] See Articles 53 and 54 of Directive (EU) 2016/680.
[77] *Ibidem*.

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

to impose limitations or bans on processing. In the view of the WP29, this attribute calls for binding powers of DPAs to warn, impose or order certain corrective actions and issue binding decisions against controllers[78].

Most Member States will have only one DPA for both the GDPR and the Directive (EU) 2016/680, but some Member States will limit the powers of their DPAs when acting under the scope of the Directive[79].

Legal remedies in Directive (EU) 2016/680:

1) Right to lodge a complaint with a supervisory authority (art. 52),
2) Right to an effective judicial remedy against a supervisory authority (art. 53),
3) Right to an effective judicial remedy against a data controller or processor (art. 54),
4) Right to be represented (art. 55)
5) The right to compensation (art. 56).

Article 55 of Directive (EU) 2016/680 provides that data subjects have „the right to mandate a not-for-profit body, organisation or association which has been properly constituted in accordance with Member State law, has statutory objectives which are in the public interest and is active in the field of protection of data subject's rights and freedoms with regard to the protection of their personal data to lodge the complaint on his or her behalf". Such provision enables not-for-profit bodies and organizations to defend data subject rights in the event of a breach. Such an organisation specializing in the field of defending data subjects already exists and provides help for those[80]. The mentioned provision may be important from the *pro bono* lawyers point of view, who specialises in data protection

[78] Opinion WP 2017/258 on some key issues of the Law Enforcement Directive (EU 2016/680). Adopted 20 November 2017.
[79] Minutes of the seventh meeting of the Commission expert group on the Regulation (EU) 2016/679 and Directive (EU) 2016/680 from 7 March 2017.
[80] For example, NOYB – European Center for Digital Rights with seat in Annagasse 8/8, 1010 Wien, Austria which was founded by Max Schrems - well known privacy activist.

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

field, as the European legislator opened a new niche for providing data subjects with legal aid in regard to prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties.

Article 56 of Directive (EU) 2016/680 provides for the compensation of persons who suffer damages after an infringement caused by an unlawful processing operation or of any act infringing national provisions adopted pursuant to Directive (EU) 2016/680. Any data subject in this matter is entitled to receive compensation from the controller or any other authority competent under Member State law. This provision is very similar to Article 19 of Framework Decision 2008/977/JHA. The former provision in Article 19 of Framework Decision 2008/977/JHA stipulated that any person who has suffered damage as a result of an unlawful processing operation or of any act incompatible with the national provisions adopted pursuant to Framework Decision 2008/977/JHA shall be entitled to receive compensation for the damage suffered from the controller or other authority competent under national law. The European Commission stated (referring to the CJEU case-law) that the access to compensation could not be based on a requirement of fault from the controller[81].

The Directive (EU) 2016/680 also instructs Member States to provide rules on the penalties applicable to violations of the provisions adopted pursuant to the Directive[82]. Unlike the Article 83 GDPR, the Directive (EU) 2016/680 does not have a provision on administrative fines, but only Article 57 which refers to 'penalties'. Recital 89 states that penalties should be imposed – but it does not refer to them as being necessarily of criminal nature.

[81] Minutes of the seventh meeting of the Commission expert group on the Regulation (EU) 2016/679 and Directive (EU) 2016/680 from 7th of March 2017.
[82] See art. 57 of Directive (EU) 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 deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

Chapter 6: Conclusions

The Review on the Directive (EU) 2016/680 leads to the general conclusion that the mentioned legislation is a positive development in comparison to Framework Decision 2008/977/JHA and has a lot in common with the GDPR. Though it should be stressed that, in order to allow effective criminal law enforcement, there are also inevitable differences. As it has been exemplified, Directive (EU) 2016/680 is *lex specialis* and aims to set specific rules for the personal data processing in criminal law, while the GDPR is *lex generalis* and does not provide effective rules for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties.

The specified goal of this report was to review Directive (EU) 2016/680 with respect to the legal professionals, one of the target groups of the INFORM project. In this context, it is important to emphasise once again that there are no legal obligations nor rights, which derive from Directive (EU) 2016/680 aiming directly at legal professionals.

Nevertheless, there are certain aspects of the Directive which may have an impact on the work of legal professionals. For instance, the right to be represented provided in Article 55 of Directive (EU) 2016/680 should be noticed. The data subject is to be equipped with the right to mandate adequate[83] not-for-profit body, organisation or association to lodge the complaint on his or her behalf and to exercise his/her rights referred to in Articles 52, 53 and 54 of Directive (EU) 2016/680. The mentioned article gives a new framework for providing data subjects with legal aid regarding prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties.

The fact that the legal professionals are not specifically addressed as a separate target group in the Directive (EU) 2016/680 does not reduce the role of legal practitioners in the field of data protection. Legal professionals acting as legal representatives of data subjects may have the obligation to protect his or her rights deriving from Directive (EU) 2016/680. Especially legal professionals who act as legal representatives of natural persons in the field of criminal law[84] will be able to provide more robust and

[83] See page 39 of this review.
[84] Prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties.

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

tailored legal services after reading this review and monitoring the rights of their client determined in Directive (EU) 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 deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

Bibliography

1) Minutes of the third meeting of the Commission expert group on the Regulation (EU) 2016/679 and Directive (EU) 2016/680, 7th of November 2016.

2) Minutes of the fifth meeting of the Commission expert group on the Regulation (EU) 2016/679 and Directive (EU) 2016/680 from 18th of January 2017

3) Minutes of the seventh meeting of the Commission expert group on the Regulation (EU) 2016/679 and Directive (EU) 2016/680 from 7th of March 2017

4) Minutes of the ninth meeting of the Commission expert group on the Regulation (EU) 2016/679 and Directive (EU) 2016/680, 4th of May 2017.

5) Article 29 Working Party Opinion WP 2017/258 on some key issues of the Law Enforcement Directive (EU 2016/680). Adopted 20 November 2017

6) Opinion 1/15 of the European Union Court of Justice on the Draft PNR Agreement between Canada and the European Union, 26 July 2017

7) Working Party on Police and Justice, The Future of Privacy. Joint contribution to the consultation of the European Commission on the legal framework for the fundamental right to protection of personal data, adopted on 01 December 2009.

8) Pajunoja, L.J. (2017) The Data Protection Directive on Police Matters 2016/680 protects privacy - The evolution of EU´s data protection law and its compatibility with the right to privacy, Master Thesis, Helsinki: University of Helsinki.

9) Bräutigam, T. The land of confusion: international data transfers between Schrems and the GDPR. T. Bräutigam & S. Miettinen, Data protection, privacy and European regulation in the digital age, p. 143-177.

10) Kuner, C. (2012) The European Commission"s Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law (2012) *Privacy and Security Law Report*.

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

11) Custers, B., Dechesne, F., Sears, A., Tani, T., Van der Hof, S. (2017) A comparison of data protection legislation and policies across the EU, *Computer Law & Security Review*, http://dx.doi.org/10.1016/j.clsr.2017.09.001.

12) Custers, B., and Vergouw, B. (2015) Promising policing technologies: Experiences, obstacles and police needs regarding law enforcement technologies, *Computer Law & Security Review*, 31, p. 518-526.

13) Bygrave, L.A. (2002) *Data Protection Law; approaching its rationale, logic and limits, Information Law*. New York: Kluwer.

Case law

1) C-101/01 Lindquist, CJEU
2) C-291/12 Schwarz v. Bochum, CJEU
3) C-582/14 Breyer v. Germany, CJEU
4) Tele2 Sverige and Watson and Others, CJEU
5) S. and Marper v. UK, ECHR
6) M.K v. France, ECHR
7) S. and Marper v. the United Kingdom, ECHR
8) Engel and others v. The Netherlands, ECHR

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

Appendix A: State of Directive (EU) 2016/680 transposition in Member States – February 2018

Country	Information on stage of implementation (including foreseen date for adoption)	Independent act or same act as GDPR
Austria	The law has been adopted by Parliament and will enter into force on 25.5.2018. The text can be found under the following link: http://www.ris.bka.gv.at/Dokumente/BgblAuth/BGBLA_2017_I_120/BGBLA_2017_I_120.pdf	Same
Belgium	• Draft law for implementing GDPR and transposing Police Directive was submitted to Government. • Following agreement at Government level, the draft law will be sent to Council of State and DPA for advice and will then be submitted to Parliament.	Same
Bulgaria		Same
Czech Republic	The draft laws were submitted to inter-ministerial consultation in August 2017 (draft was submitted to the Cabinet in the end of October 2017 and it will be submitted to the Parliament in April).	Independent
Cyprus	Working Group with Ministry and DPA to prepare the legislation. The objective is to have public consultation and subsequently the draft to be sent to Parliament before end of this year	Independent

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

Germany	- The restructured Federal Data Protection Act ("Bundesdatenschutzgesetz"; Article 1 of the "Datenschutz-Anpassungs- und -Umsetzungsgesetz EU") including a section specifically dedicated to the DPD implementation (part 3) will come into effect on May 25, 2018. - ongoing legislative implementation efforts on the state (Länder; due to the distribution of competencies in the federal system largely responsible for the police and justice sector) level with varying progress (there are indications that 3 of the 16 states will have implanting rules in effect by the end of May 2018); the Federal level is closely monitoring those efforts but has no power to influence the process.	One federal law, complemented by legislation covering agencies/authorities that process data under the umbrella of the DPD designed to meet their special needs (e. g. Federal Criminal Police Office, BKA; the restructured BKA Act coming into effect on May 25, 2018). Further implementing legislation in that sense will have to be done with regard to the Federal Police, the Federal Customs Criminal Office and the provisions regulation the criminal procedure (
Denmark	The transposition law adopted on 27 April and entered into force on 1 May 2017.	Independent
Greece	Currently at the level of a working group.	Same
Estonia	Draft law should be finalised and presented to the Government in the beginning of 2018, with a view of adoption by the Parliament in Q1 2018.	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 deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

Spain	Working party established to prepare the transposition/adaptation of national laws. A first draft of the transposition law due for September. No timetable for Parliament yet.	
France	• Working group composed by relevant parts of the Ministry, law professors and CNIL – 7 meetings took place. Working group has completed its work. • Consultation with several concerned Ministries (research, archives, home affairs, etc.) is over. • Proposal to new Justice Minister for policy choices on situations such as Art 8, 89 took place in September 2017. • Draft law was submitted for opinion of Conseil d'Etat and CNIL. • Draft law was submitted to Parliament in December 2017. The first reading in Assembly was concluded on 13 February 2018. The process in Senate is expected to be finalized by end of March 2018. Draft law can be found at: http://www.assemblee-nationale.fr/15/dossiers/donnees_personnelles_protection.asp	Same
Finland	Public consultation was closed, and the draft law was presented in October for the adoption by the Parliament. It should be adopted before May 2018.	Independent
Hungary	• Work on draft law for reviewing the provisions on the procedures conducted by the DPA and introducing other changes required by the GDPR • Draft law covers both GDPR and Police Directive • Consultations with stakeholders on the horizontal issues were carried out (started in August closed in September) • Consultation with stakeholders on sector-specific laws is still ongoing • Government discussed the draft law and decided on the need of further examinations (concerning sectoral laws)	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 deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

	• A high-level consultation group was established with the participation of relevant stakeholders (bank, insurance, telecom industry) as well as the responsible line ministries and authorities including the DPA aiming at awareness-raising, identifying potential difficulties in the course of implementation and application	
Croatia	The draft law will be presented by 26 March to the approval of the Government and then sent to the Parliament.	Independent

Ireland	• The General Scheme has undergone pre-legislative scrutiny by the relevant Parliamentary Committee. The Bill was drafted by the Office of Parliamentary Counsel.
	• The Data Protection Bill 2018 (draft law) was submitted to Parliament on 30 January. Discussions commenced already in Parliament on 8 February. The Bill will—
	  • Establish the Data Protection Commission (with up to three Commissioners) to replace the Data Protection Commissioner;
	  • give further effect to the GDPR in areas where national law is permitted;
	  • transpose the law enforcement Directive;
	  • provide for enforcement of both the GDPR and Directive;
	  • amend cross-references to existing data protection law in various Acts and regulations.
	• The bill is expected to be adopted by May 2018.
	Draft bill can be found at: http://www.oireachtas.ie/viewdoc.asp?DocID=37646&&CatID=59
		Same

Italy	Draft law may be passed in March as a Governmental Decree (delegation from the Parliament)	Independent

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

Lithuania	Public consultation –June Draft law submitted to Government in March. Draft law submitted to Parliament in April.	Independent
Luxembourg	The bill submitted to the Parliament in August and the legislative process might take until May 2018.	Independent
Latvia	The draft was submitted to the Government in October. It was submitted to the Parliament in the end of February, for adoption before the transposition deadline.	Independent
Malta	The first draft law is ready, but not publicly available. No precise time-frame.	Independent
Netherlands	The draft bill has been submitted Parliament for the adoption before the deadline. The implementing by-laws have been sent to the Council of State.	Independent
Poland	Should have the first draft ready soon and launch governmental inter-service consultations afterwards.	
Portugal		
Romania	Task force Ministers and DPA to implementing GDPR and Directive An interministerial memorandum adopted regarding the calendar 3 draft laws: DPA; implementing GDPR; transposing Directive. Public consultation till August. Draft law submitted to Government end August	Independent

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

	Draft law submitted to Parliament – mid September	
Sweden	A committee of inquiry presented a report in April 2017. The report has been sent to consultation bodies and a draft bill will be prepared and send to the Parliament in the early spring 2018.	Independent
Slovenia	• Considering a type of "Omnibus act" to amend a number of sector laws plus a draft law on GDPR • Draft law will go through public consultation from October to 10 November. Draft general law to be submitted to Parliament by beginning of March 2018.	Same
Slovakia	• New Act on Protection of Personal Data is signed by the President. The law has been published in the Collection of Laws (the official instrument) under the number 18/2018, and it will enter into force on 25 May 2018. • It will repeal existing Act on protection of personal Data • New Act on Protection of Personal Data: 1. applies to the processing that are not covered by GDPR, 2. applies in certain parts also to processing covered by GDPR	Same
United Kingdom	The UK's Data Protection Bill and explanatory notes was introduced in Parliament on 13/09 and published on 14/09: https://www.gov.uk/government/collections/data-protection-bill-2017 The bill is expected to be adopted by May 2018. Its progress can be followed online.	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 deliverable are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Commission.

Switzerland	The bill is now under parliamentary scrutiny. There will be some specific provisions in the criminal code and the criminal procedural law. In its data protection reform, the transposition of the Directive has a priority as Schengen acquis.	Independent

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