

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

D2.2: Review report on Directive 2016/680  
aimed at the judiciary

Lead partner: eLaw - University of Leiden



<b>Project co-funded by the European Commission within the JUST Programme</b>		
<b>Dissemination Level:</b>		
<b>PU</b>	Public	X
<b>CO</b>	Confidential, only for members of the consortium (including the Commission Services)	
<b>EU-RES</b>	Classified Information: RESTREINT UE (Commission Decision 2005/444/EC)	
<b>EU-CON</b>	Classified Information: CONFIDENTIEL UE (Commission Decision 2005/444/EC)	
<b>EU-SEC</b>	Classified Information: SECRET UE (Commission Decision 2005/444/EC)	
<b>Document version control:</b>		
<b>Version 1</b>	Originated by: Bart Custers and Georgios Stathis eLaw, Leiden University	19/01/2018
<b>Version 1</b>	Reviewed by: Matthias Eichfeld, University of Göttingen	25/01/2018
<b>Version 1</b>	Reviewed by: George Dimitrov, Law and Internet Foundation	31/02/2018
<b>Version 2</b>	Updated by: Bart Custers, eLaw, Leiden University	23/03/2018
<b>Version 2</b>	Reviewed by: George Dimitrov, Law and Internet Foundation	27/03/2018
<b>Version 2</b>	Updated by: Bart Custers, eLaw, Leiden University	11/04/2018
<b>Version 2</b>	Reviewed by: George Dimitrov, Law and Internet Foundation	13/04/2018
<b>Version 2</b>	Reviewed by: Matthias Eichfeld, University of Göttingen	16/04/2018



## **INFORM**

INFORM<sup>1</sup> is an 18-month project, funded by the European Commission under the Justice (JUST) Programme 2014-2020, introducing to the judiciary, legal practitioners, and court staff to the new data protection legislation provisions. The project is designed to contribute to the effective and coherent application of the General Data Protection Regulation (GDPR) and to facilitate the implementation and practical application of Directive (EU) 2016/680. Under the coordination of Law and Internet Foundation, the project will cater to the training needs of the judiciary, legal practitioners, and court staff and present them with a comprehensive overview of the new EU data protection legislation. The project concept is to reach the judiciary, legal practitioners and court staff utilising train-the-trainer approach. INFORM will engage trainers, empowering them with tailor-made materials and customised training methodology.

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.

---

<sup>1</sup> [www.inform-project.eu](http://www.inform-project.eu).



## Executive summary

In April 2016, EU Directive 2016/680 was adopted by the European Parliament and the Council, together with the General Data Protection Regulation (GDPR). This Directive 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. In short, that means personal data processing by all organisation involved in the criminal law chain, such as the police, public prosecution services, courts and the prison system. This report reviews Directive 2016/680 for a specific target group, the judiciary.

The judiciary has two distinct roles regarding Directive 2016/680. First, as a competent authority (Article 3.7), the judiciary will have to apply the Directive (or rather its implementation in national legislation) in cases on which it is working. Second, institutions of the judiciary may also be considered as a data controller (Article 3.8) of the personal data. Both roles may depend on the way the judiciary is organised in a particular member state.

In this report an overview of the history and background of the Directive provided, its material scope and terminology used are examined and a structured review of its main provisions is provided. These provisions concern the principles for the fair processing of personal data, data subject rights, data controller obligations, international data transfers, independent supervision and cooperation, and remedies, liability and penalties.

When reviewing Directive 2016/680 it is apparent that there is a lot of overlap with the GDPR, but there are also a number of noticeable differences. Directive 2016/680 aims to set more specific rules for the processing of personal data in criminal law, since the GDPR does not always provide sufficiently adequate and detailed rules for the context of criminal law. Directive 2016/680 tries to provide a more contextualised balance. At the same time, on a more general level, this Directive constitutes a further harmonisation of criminal law across EU member states, facilitating the cooperation within the EU in the area of criminal law.



The goal of this report is to review Directive 2016/680 specifically for the judiciary, one of the target groups of the Directive. However, the review shows that there are almost no special provisions for the judiciary within the Directive. The biggest exception can be found in Article 45, where it is stated that national Data Protection Authorities are not competent for the supervision of data processing of courts (when acting in their judicial capacity). Furthermore, member states may provide for their Data Protection Authorities not to be competent to supervise data processing of other independent judicial authorities.

The Directive is highly relevant for both roles of the judiciary, as the judiciary is processing (sometimes particularly sensitive) personal data that are extremely relevant in the prosecution and sentencing of crimes (both as clues in criminal investigation and as evidence in courts, such as witness statements) and, as such, should be treated according to the rules. This will ensure that all rights of suspects and other data subjects that may be involved in criminal law cases (such as witnesses, victims, etc.) are adequately protected.



## Table of Contents

Executive summary .....	4
Table of Contents.....	6
Chapter 1: Introduction.....	8
1.1 EU Directive 2016/680 .....	8
1.2 History and background .....	9
1.3 Aims of this report .....	12
1.4 Structure of this report .....	13
Chapter 2: Material scope and terminology.....	14
Chapter 3: Data processing by the judiciary.....	18
Chapter 4: Principles for data processing .....	20
Chapter 5: Data subject rights and data controller obligations .....	23
5.1 Data subject rights.....	23
5.2 Data controller obligations.....	25
Chapter 6: Data transfers .....	28
Chapter 7: Supervision, cooperation and liability.....	30
7.1 Independent supervision and cooperation.....	30
7.2 Remedies, liability and penalties .....	31
Chapter 8: Conclusions.....	33
Bibliography .....	34



Appendix A: List of training authorities for the judiciary .....37



## Chapter 1: Introduction

### 1.1 EU Directive 2016/680

In April 2016, together with the General Data Protection Regulation (GDPR), EU Directive 2016/680 was adopted by the European Parliament and the Council. This Directive<sup>2</sup> 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. In short that means personal data processing by all organisation involved in the criminal law chain, such as the police, public prosecution services, courts and the prison system. The GDPR is the *lex generalis*, whereas Directive 2016/680 (‘the Directive’) can be considered as a *lex specialis* for personal data in criminal law. The GDPR is an EU regulation and, as such, directly binding for all EU citizens, companies and government organisations, whereas the Directive requires (mandatory) implementation into national legislation of member states. The deadline for this implementation is May 2018.

Companies and government institutions are very busy with the General Data Protection Regulation (GDPR) that will be in force as of May 2018. The GDPR replaces EU Directive 95/46/EC on the protection of personal data (in short the Data Protection Directive, DPD)<sup>3</sup> and contains several new elements for data subjects (such as a right to data portability and the right to be forgotten) and new obligations for data controllers (such as data breach notifications, mandatory data protection officers and concepts like Data Protection Impact Assessments and Data Protection by Design and by Default).<sup>4</sup> Another very important aspect of the GDPR is the possibility for supervisory authorities to impose administrative fines in the case of non-compliance. These fines can be considerable, to a maximum of 10 or 20 million euros (depending on the type of 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. This obviously raises worries for organisations on whether they are completely compliant with the GDPR.

---

<sup>2</sup> DIRECTIVE (EU) 2016/680 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

<sup>3</sup> DIRECTIVE (EU) 95/46/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

<sup>4</sup> WP29 (2017) Opinion WP 2017/258 on some key issues of the Law Enforcement Directive (EU 2016/680). Adopted 20 November 2017.





Much less well-known is the act that together with the GDPR the EU published Directive 2016/680 on the processing of personal data in criminal law.<sup>5</sup> This Directive focuses on the processing of personal data by organisations in the criminal law chain (e.g., the police, public prosecution services, courts and the prison system) within their legal tasks and competences (e.g., preventing, investigating, prosecuting and sentencing crimes and executing criminal penalties. For instance, when a law enforcement agency or a court processes personal data of their employees to pay the wages, the GDPR applies, since these data are not directly related to the task of criminal investigation. As will be explained in the next Chapter, the focus is on so-called competent authorities, which may not only include public authorities but also other bodies and entities entrusted by national law to exercise public authority and public powers.

In short, Directive 2016/680 aims to set more specific rules for the processing in personal data in criminal law. This domain is explicitly excluded from the scope of the GDPR (see article 2.1.d of the GDPR). Although information rights exist in criminal law, as will be shown in this report, the balance between the needs of criminal law chain organisations and the protection of data subjects is slightly different in criminal law than regulated by the GDPR. Directive 2016/680 tries to provide this more contextualised balance. At the same time, on a more general level, the Directive constitutes a further harmonisation of criminal law across EU member states, facilitating the cooperation within the EU in the area of criminal law. As such, the directive is not only about ensuring the same level of protection for natural persons, but also about the free movement of data (see Recital 15).

## 1.2 History and background

The history of Directive 2016/680 runs mostly parallel with that of the GDPR. The GDPR mainly builds on and extends the EU Data Protection Directive (DPD) from 1995.<sup>6</sup> This Directive, in turn,

---

<sup>5</sup> This Directive is sometimes referred to as the Police Directive, see, for instance, COM (2017) Exchanging and Protecting Personal Data in a Globalised World, [https://ec.europa.eu/newsroom/document.cfm?doc\\_id=41157](https://ec.europa.eu/newsroom/document.cfm?doc_id=41157). However, this labelling is not entirely correct, since the Directive also addresses other authorities in the criminal law chain than the police. The organization of the criminal law chain is not harmonized across all EU member states and, as such, may depend on the legal system of each member state. But, in general, the police is a separate organization, apart from the public prosecution services, the courts and the prison system.

<sup>6</sup> For further reading, see Bygrave, L.A. (2002) Data Protection Law; approaching its rationale, logic and limits, Information Law; 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*; Hornung G. (2012) A General Data Protection Regulation for Europe? Light and Shade in the Commission's Draft of 25 January 2012, 9 *SCRIPTed* 64-81. Series 10, Den Haag: Kluwer Law International.



was mostly based on the provisions in Convention 108 of the Council of Europe (also referred to as the Treaty of Strasbourg) from 1981.<sup>7</sup> The Council of Europe also published a recommendation that supplements Convention 108 for the use of personal data by the police in 1987.<sup>8</sup> In this recommendation, it is further specified who has access to police data, under which conditions police data can be transferred to authorities in third countries, how data subjects can exercise their data protection rights and how independent supervision is organized. These recommendations, however, are not legally binding and many member states have not fully implemented them.

Since the processing of criminal law data is beyond the scope of Directive 95/46/EC, there was no harmonization within the EU in this domain for a long time.<sup>9</sup> After the terrorist attacks of September 11<sup>th</sup> 2001 in the United States, the European Parliament repeatedly requested a legal instrument for the so-called third pillar of the European Union, on Police and Judicial Co-operation in Criminal Matters.<sup>10</sup> However, only little progress was made.<sup>11</sup> Only in 2008 the EU published Framework Decision 2008/977/JHA on the protection of personal data processing in the framework of police and judicial cooperation in criminal matters.<sup>12</sup> This Framework Decision is also based on the principles in Convention 108 and the Data Protection Directive. National security is beyond the scope of this framework decision. The aim of the framework decision is, on the one hand, the protection of personal data that are processed for the prevention, investigation, detection and prosecution of crimes and the execution of criminal penalties and, on the other hand, the facilitation and simplification of police and judicial cooperation between member states.

Finally, a series of legal instruments should be mentioned that aim to advance the cooperation and sharing of information between member states, such as the Prüm Treaty<sup>13</sup> (for exchanging DNA data, fingerprints and traffic data), the Schengen Information System<sup>14</sup> (SIS, for international criminal investigation information), the Visa Information System<sup>15</sup> (VIS, for visa data, including biometrical

---

<sup>7</sup> Council of Europe (1981) Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, No. 108, 28.01.1981.

<sup>8</sup> Council of Europe (1987) Police Data Recommendation Rec(87)15, 17.9.1987.

<sup>9</sup> 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.

<sup>10</sup> With the Treaty of Lisbon the official pillar structure of the EU was abandoned in 2009.

<sup>11</sup> Gonzales Fuster, G. (2014) *The Emergence of Personal Data Protection as a Fundamental Right of the EU*. Heidelberg: Springer, p. 220.

<sup>12</sup> Europese Raad (2008) Framework Decision 2008/977/JHA, 27.11.2008

<sup>13</sup> EU Council Decision 2008/615/JHA; Prüm Decision, 23.6.2008.

<sup>14</sup> EU Council Decision 2007/533/JHA, SIS-II, 12.6.2007.

<sup>15</sup> EU Regulation 767/2008, VIS Regulation, 9.7.2008.



data), and the Customs Information System (CIS).<sup>16</sup> Also the institutional regulations for Europol, Eurosur and Eurojust contain provisions for the exchange of criminal law information.

In 2012 the European Commission presented the first draft for a Directive that would harmonize the processing of personal data in criminal law matters.<sup>17</sup> After that, a debate started between the European Parliament, the Commission and the Council, which took three years. In 2016, the legislative proposal was adopted, after amendments, in its current version as EU Directive 2016/680. In this Directive the deadline for implementation in national legislation is two years, with a final deadline in May 2018. Directive 2016/680 repeals the current Framework Decision 2008/977/JHA as of that date. It should be mentioned that the scope of the Framework Decision is limited to processing data that are transferred to other member states, whereas the scope of the Directive also includes the processing of criminal law data for domestic purposes.<sup>18</sup>

The aim of Directive 2016/680 is two-folded: on the one hand, it ensures the protection of personal data that are processed for the prevention, investigation, detection and prosecution of crimes and the execution of criminal penalties and, on the other hand, the facilitation and simplification of police and judicial cooperation between member states and, more in general, the effectively addressing on crime (see also Recital 15). This two-folded approach is similar to that of the GDPR and to the previously mentioned framework decision.

The most important differences between, on the one hand, the general legal instruments for the protection of personal data (Convention 108, the Data Protection Directive and the GDPR) and, on the other hand sector-specific legal instruments for the protection of criminal law data (Recommendation 87/15, Framework Decision 2008/977/JHA and Directive 2016/680) are always (roughly speaking) the same: first, the scope and targeted audiences are different, second, specific data subject rights are somewhat more restricted in criminal law matters and, third, the criminal law provisions offer sometimes a bit more detail.

---

<sup>16</sup> EU Council Decision 2009/917/JHA.

<sup>17</sup> <http://eur-lex.europa.eu/legal-content/NL/TXT/PDF/?uri=CELEX:52012PC0010&from=en> COM(2012) 9 Final.

<sup>18</sup> Salami, E. A. (2017) The Impact of Directive (EU) 2016/680 on 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 on the Existing Privacy Regime. <http://dx.doi.org/10.2139/ssrn.2912449>.



### 1.3 Aims of this report

In order to ensure the new data protection laws are sufficiently promoted and properly implemented and applied, the European Commission has initiated several calls for proposals. The INFORM project (INtroduction of the data protection reFORM to the judicial system) is a proposal that also contributes to the further promotion, implementation and application of the GDPR and Directive 2016/680, with a specific focus on the judiciary as a target audience. The aim of the INFORM project is to provide judicial training for trainers from all EU member states. This report, Deliverable D2.2 of the INFORM project, is part of Work Package 2, in which the new EU data protection laws are reviewed and training materials are developed. In the INFORM project, three different target groups are distinguished within the judicial system: the judiciary (including judges and public prosecutors),<sup>19</sup> legal practitioners (including lawyers) and court staff. This Deliverable, D2.2, reviews Directive 2016/680 for the judiciary. For a review of the GDPR for the judiciary, see D2.1. For a review of Directive 2016/680 for legal practitioners or court staff, see D2.5 and D2.8 respectively.

Note that the judiciary has two distinct roles regarding Directive 2016/680. First, the judiciary will have to apply the national laws implementing the Directive in cases on which it is working. For instance, public prosecutors may have to identify cases in which provisions of the Directive are violated and decide whether and how to prosecute such cases. Judges and courts may have to determine in specific cases brought before them whether national laws implementing the Directive were not complied with and to decide on their rulings accordingly. For instance, the transposition of Article 57 of the Directive in national law means that there will be rules on penalties applicable to infringement of the provisions implemented in national legislation pursuant to the Directive.<sup>20</sup> Second, the judiciary may also be considered as a controller of personal data according to the Directive. As such, the judiciary itself also must fully comply with the provisions in the Directive, or rather in the national laws implementing the Directive, including adequate observation of data subject rights and compliance with data controller obligations. In a centralised system (such as Bulgaria) the Supreme Judicial Council is the data controller, whereas the courts are data processors. In a decentralised system (such as the Netherlands), the courts are the data controllers. For both roles, the judiciary should have an in-depth and accurate knowledge of Directive 2016/680. For this reason, both roles of the judiciary are within

---

<sup>19</sup> The scope and definition of the judiciary are discussed in Deliverable D2.1.

<sup>20</sup> It remains to be seen how member states will implement these provisions in national law. There may be differences in choices. For instance, some countries may decide to establish separate authorities within the judicial system in order to ensure the right balance between the executive and judicial powers (see also Recital 20 of the GDPR).



scope of the INFORM project and this report. Chapter 3 will explicitly deal with the role of the judiciary as a data controller.

This review of Directive 2016/680 for the judiciary basically involves a general description of the history and background of the Directive and a chapter-by-chapter explanation and elaboration of the (provisions in the) Directive. Many provisions in the Directive are not specifically aimed at the judiciary, but, more in general, to all organisations in the criminal law chain. However, where the judiciary is specifically addressed and/or where the situation differs for the judiciary compared to other criminal law organisations, this is elaborated upon. Furthermore, by providing specific examples in the context of the judiciary, further explanation is provided to illustrate the meaning and impact of the Directive for the judiciary.

The information provided in this report is the basis for the training materials that are developed in the INFORM project. However, it should be noted that this report is not intended as training material itself. For more information on the training materials and the actual trainings, such as workshops, e-learning programs and information days, see the INFORM website at: <http://informproject.eu/>

## 1.4 Structure of this report

In this report, the contents of Directive 2016/680 are reviewed for the judiciary, which is a specific target group distinguished within the INFORM project. The structure of this report follows the chapter structure of the Directive. Chapter 2 examines the material scope of the Directive and discusses concepts like personal data and data processing. Chapter 3 elaborates on the role of the judiciary as a data controller. Chapter 4 discusses the fundamental principles for the processing of personal data. Chapter 5 elaborates on respectively the data subject rights and the data controller obligations provided by the Directive. Chapter 6 focuses on the transfer of personal data to third countries. Chapter 7 focuses on independent supervision and cooperation and on remedies, liability and penalties. Chapter 8 provides conclusions.



## Chapter 2: Material scope and terminology

Directive 2016/680 and the GDPR are related to each other as a *lex specialis* versus a *lex generalis*: the GDPR applies to the processing of personal data in general but is set aside for the processing of personal data in a criminal law context, for which the specific rules of the Directive apply (see Article 2.2.d of the GDPR). The scope and the objectives of the Directive are presented in its first chapter (articles 1-3), together with a set of definitions explaining the terminology used. As such, the first chapter of the Directive lays the foundations for the Directive. It recognizes the right for the protection of personal data as a fundamental right and freedom of natural persons and it lays the basis for a single market by ensuring the protection of the transfer of data among member states.

The Directive focuses on data processing by so-called competent authorities, which is defined in art. 3.7. **Competent authorities** include (a) any public authority competent for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security and (b) any other body or entity entrusted by Member State law to exercise public authority and public powers for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security. Hence, competent authorities, may not only include public authorities, such as the judicial authorities, the police or other law enforcement authorities, but also other bodies and entities entrusted by national law to exercise public authority and public powers (Recital 11). These other bodies are usually under the scope of the GDPR, also when they collect or process personal data to comply with a legal obligation to which they are subjected. For example, for the purposes of investigation detection or prosecution of criminal offences financial institutions retain certain personal data which are processed by them, and provide those personal data only to the competent national authorities in specific cases and in accordance with national law. A body or entity which processes personal data on behalf of such authorities within the scope of the Directive should be bound by a contract or other legal act and by the provisions applicable to processors pursuant to this Directive, while the application of GDPR remains unaffected for the processing of personal data by the processor outside the scope of Directive 2016/680.

The scope of the Directive is limited to the processing of personal data by the competent authorities for the **specific purposes** of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties (art. 1 and 2). This includes the safeguarding against and the prevention of threats to public security (see also Recital 11). As such, it should be noted that





not all personal data processed by law enforcement agencies and the judiciary is within the scope of the Directive. For instance, when law enforcement agencies or the judiciary are processing personnel data regarding their staff, for instance, for paying wages or assessing employee performance, the GDPR applies rather than the Directive. The GDPR is also applicable for personal data processing regarding borders, migration and asylum. Only when data are processed in criminal procedures by these organizations, they are within the scope of the Directive. Also, when others that the competent authorities collect and process personal data on criminal cases, these data are within the scope of the GDPR rather than the Directive. For instance, when a professor in criminal law or criminology wants to study organized crime and receives a copy of some criminal files from the judiciary, the personal data in these files kept by the professor are in the scope of the GDPR rather than the Directive. Similarly, when a private investigator (‘private detective’) or a journalist starts digging into a crime, he may collect personal data on suspects, criminals, witnesses, etc. These personal data, kept by private investigators or journalists are within the scope of the GDPR rather than the Directive.

When a body or entity collects and processes personal data in order to comply with a legal obligation to which it is subject, the GDPR applies. For example, for the purposes of investigation, detection or prosecution of criminal offences, financial institutions retain certain personal data which are processed by them, and provide those personal data only to the competent national authorities in specific cases and in accordance with national law (see Recital 11). These financial institutions are not considered to be competent authorities in the meaning of the directive and, therefore, are within the scope of the GDPR rather than the Directive. A body or entity which processes personal data on behalf of such authorities within the scope of the Directive should be bound by a contract or other legal act and by the provisions applicable to processors pursuant to the Directive, while the application of the GDPR remains unaffected for the processing of personal data by the processor outside the scope of the Directive. Typical examples may be tax and customs authorities, financial investigation units, independent administrative authorities, or financial market authorities responsible for the regulation and supervision of securities markets (see Recital 22).

Both data used on crimes that have already taken place (for instance, data regarding crime reconstructions and evidence for in courts) and data used on crimes that still might take place (for instance, crime prediction models that police agencies use to prevent crime)<sup>21</sup> are within the scope of the Directive. The data may relate to crimes, but also to suspects, criminals, victims, witnesses, testifying law enforcement officers, and police informants. In case of crime prevention, there may be

---

<sup>21</sup> See also Recital 26.



suspects involved (i.e., those preparing a crime), without a completed criminal act (as it was still in preparation).<sup>22</sup> The crimes may be directed against specific victims, but in some cases there may not be a specific victim. Typical examples include the possession of illegal contraband or recreational drug use.

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

All natural persons of whom personal data are processed within criminal law are within the scope of the Directive, regardless of nationality or residence. The Directive does not apply to the processing of personal by EU institutions, bodies, offices and agencies (art. 2.3.a). Directive

Article 4 of the Directive provides a list of definitions. The definition of personal data is perhaps the most important one.<sup>23</sup> Similar to the GDPR text, personal data are defined as any information relating to an identified or identifiable<sup>24</sup> natural person (the data subject). This means that data relating to legal persons (even when they are involved in criminal matters) are not within the scope of the Directive. Also, the personal data of deceased people are beyond the scope of the Directive, although it should be noted that there may be other legislation that prevents disclosure of personal data of deceased people.

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. Chapter 3 of this report will elaborate on personal data processing by the judiciary (i.e., the judiciary in its role of data controller). It should be noted that some types of data processing, such as anonymization (see also Article 3.5 of the Directive), may transform personal data into non-personal data, putting it beyond the reach of the Directive. Recital 20 of the Directive explicitly mentions 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 as regards personal data contained in a judicial

---

<sup>22</sup> Note that preparing serious crimes is a punishable offence (and hence a crime in itself) in most jurisdictions.

<sup>23</sup> See also WP29 (2018) Guidelines on Personal data breach notification under Regulation 2016/679. Article 29 Working Party, 6 February 2018; WP29 (2018) Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679. Article 29 Working Party, 6 February 2018;

<sup>24</sup> Identifiability may depend on the amount of time, effort and costs involved. For more on absolute or relative identifiability of a person, see also ECJ, Case C-582/14 (Breyer/Germany).





decision or in records in relation to criminal proceedings. This means that member states may transpose the Directive in their national criminal procedural law, but they cannot derogate from it.

The directive explicitly mentions special categories of personal data in Article 10. These are personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation. The GDPR also mentions special categories of data, but the Directive much more defined the special categories of personal data. In criminal law, some specific types of data may be useful to process for the competent authorities (including the judiciary), such as genetic data (in forensic DNA research), biometric data (including genetic data and fingerprints, to identify suspects) and data concerning health (for instance expert reports on the mental health of suspects to determine criminal liability).<sup>25</sup> These types of data are specifically mentioned in Article 3 of the Directive and may be useful in criminal investigations (finding clues about what happened and pointers for suspects and witnesses) and in criminal prosecution and sentencing (providing evidence in courts). In Article 10 of the Directive these types of data are defined as special categories of personal data (sensitive data) that can only be processed when provided by law, when strictly necessary and subject to appropriate safeguards.<sup>26</sup>

---

<sup>25</sup> Custers B.H.M. & Prinsen M.M. (2010), *Introduction to Forensics*. In: Herzog-Evans M (red.) *Transnational Criminology Manual*. Tilburg: Wolf Legal Publishers. 15-34.

<sup>26</sup> See also WP29 (2017) Opinion WP 2017/258 on some key issues of the Law Enforcement Directive (EU 2016/680). Adopted 20 November 2017.



## Chapter 3: Data processing by the judiciary

As indicated in Chapter 1, the judiciary can be both a competent authority according to Article 3.7 of the Directive and a data controller as defined in Article 3.8 of the Directive. In this chapter we focus on the second role, in which the judiciary is processing personal data. In order to determine whether a court or a public prosecution service processes personal data, the first step is to assess whether the data that are collected and processed are personal data. When data relate to an identified or identifiable natural person, they are personal data. This includes names, identification numbers and biometric data (including facial images, fingerprints, DNA, retina scans, etc.). Obviously the data have to be of sufficient quality. For instance, half a fingerprint or damaged DNA samples may not be sufficient to extract digital profiles for further matching.

It is important to note the difference between ‘identified’ and ‘identifiable’. Identifying a person is usually about ‘singling out’ individuals from the masses. As such, identifying characteristics and attributes, such as names, social security numbers or identity cards, concentrate on unique characteristics of people. However, the usefulness of such identifiers may depend the context in which they are used. A name or a face may usually be sufficient for people to identify family and friends, but for law enforcement, this may not work when some names are more prevalent or people look similar. The question then becomes, which characteristics (or combination of characteristics) can be used to identify individuals. For this, it is not relevant that individuals are actually identified, but rather that they could be identified, i.e., whether they are identifiable. Identifiability obviously depends on the amount of time, effort and resources available. When a reasonable amount of time, effort and resources would enable identifying a person, the data subject is considered to be identifiable and, as such, the data is considered to be personal data. For instance, a facial image of a recognizable person is personal data for the police, even if it is unknown who the person is (for instance, nobody has seen the person before, nobody recognises the person or the person’s name is unknown). It is sufficient that a person might be identifiable by his or her family, friends, etc.

By this account, also location data, online identifiers and all kinds of other attributes (or combinations thereof) may be considered personal data.<sup>27</sup> For instance, GPS data, IP addresses or vehicle license plates are personal data, because they can be related to natural persons, perhaps not by the average

---

<sup>27</sup> Note that anonymization has to be strong to prevent recombination of data with personal identifiers, see Ohm, P. (2010) Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization. *UCLA Law Review* 57, 1701–1765.



citizen, but certainly by others, such as the GPS service provider, the Internet service provider and the national authorities respectively.

Anonymous data and data of deceased people are not within the definition of personal data. Hence, when competent authorities consider the provisions in the Directive as too restrictive for their aims, they may consider anonymizing the data. Typical examples may be crime statistics and profiling. For these purposes, anonymised data may be sufficient to work with. The advantage of anonymization (or sometimes pseudonymization, at least when it breaks linkability) of data, which is encouraged in the Directive, is that it provides further security safeguards. In general, in the case of data breaches, the impact is less when linkability is limited (so-called compartmentalization) than when it concerns personal data.

The judiciary can be involved in a wide range of data processing activities. It is important to note that data processing according to the Directive also includes activities that in normal language are not considered as such. For instance, data collection, consultation and dissemination are also types of data processing. When the police transfers a case file to the public prosecutor, this is a type of data collection (and hence a type of data processing) of the prosecutor. As such, data collection can be either passive or active. Having cameras in court rooms is a type of data processing because personal data is processed. Furthermore, the language in the Directive is not always in line with the technological jargon: for instance, in information technology, data storage is quite something different than data processing, but in the Directive data storage is considered to be a type of data processing.

It is possible that the judiciary as a data controller outsources some of its data processing activities to a data processor. Although it is not always likely, mainly because of the confidentiality of the data, this may happen, for instance, because the data may need further analysis from experts. In such cases, the data controller remains responsible for all the activities of the data processor. In order to mitigate compliance risks, it is usually recommended to perform so-called Privacy Impact Assessments (PIAs), which the GDPR and the Directive refer to as Data Protection Impact Assessments.<sup>28</sup> These are risk assessments that assess in systematic ways the privacy and data protection risks of types of data processing, in particular when using new technologies. According to the Directive, a Data Protection Impact Assessment may be required when the data processing is likely to result in a high risk to the rights and freedoms of natural persons (Article 27). With the results of such a (privacy) risk assessment, risk mitigating measures can be taken, including adequate security safeguards, role-based access, limited storage times, anonymization or pseudonymization, etc.

---

<sup>28</sup> For more details, see Wright, D., and Hert, P. de (2012), *Privacy Impact Assessment*, Heidelberg: Springer.



## Chapter 4: Principles for data processing

The main substance of both the GDPR and the Directive are the so-called fair principles for the processing of personal data. These provide procedural rules and guidance for the processing of personal data, in order to ensure fairness. The fair principles for the processing of personal data include fair and lawful processing, purpose limitation, accuracy of the data, adequate security safeguards and responsibility of data controllers. The principle of transparency is observed as much as possible, but there are differences in the phrasing of the GDPR and the Directive, because full transparency may not always be realistic in criminal law, as it may interfere with or frustrate ongoing criminal investigations.

The main principles for data processing are based on those in Convention 108 and the Data Protection Directive (see Chapter 1) and include:<sup>29</sup>

- Lawfulness and fairness (art. 4.1.a)
- Purpose specification and limitation (art. 4.1.b)
- Data minimisation (art. 4.1.c)
- Accuracy (art. 4.1.d)
- Storage limitation (art. 4.1.e)
- Appropriate security (art. 4.1.f)
- Accountability (art. 4.4)

According to Recital 29, personal data should be collected for specified, explicit and legitimate purposes within the scope of the Directive and should not be processed for purposes incompatible with the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.<sup>30</sup> In contrast with the GDPR, the Directive does not provide an exhaustive list of legal bases for the lawfulness of personal data processing. The GDPR (art. 6) states that the processing of personal data is only allowed if one of the six legal bases mentioned is applicable. This closed system

---

<sup>29</sup> For further reading, see R. Gellman (2012) *Fair Information Practices: A Basic History*, available at <http://bobgellman.com/rg-docs/rg-FIPShistory.pdf>.

<sup>30</sup> If personal data are processed by the same or another controller for a purpose within the scope of the Directive other than that for which it has been collected, such processing should be permitted under the condition that such processing is authorised in accordance with applicable legal provisions and is necessary for and proportionate to that other purpose.



includes the following options: consent, contractual basis, legal obligation, vital interests, public interest or legitimate interests. The Directive does require a legal basis for the processing of personal data in criminal law in Article 8, but contains no list of legal bases like in the GDPR.

A second difference between the GDPR and the Directive exists in time limits for storage and review (art. 5 of the Directive Directive). The GDPR does not mention any time limits at all,<sup>31</sup> but the Directive states that member states should 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. Article 5.1.e of the GDPR states that personal data should be kept no longer than necessary, but does not mention a number of days, months or years. The Article 29 Working Party issued an opinion that argues that time limits should be differentiated.<sup>32</sup>

A third difference between the GDPR and the Directive is that the Directive explicitly distinguishes different categories of data subjects (offering more detail than the GDPR in this respect). In art 6 of the Directive, a distinction is made between suspects, persons convicted of a crime, victims and other parties to a criminal offence (including witnesses). Data controllers should make a clear distinction between the personal data of different categories of data subjects.

**Example: consent**

The company B&G B.V. is an Intelligence software company operating in the EU with HQ in Leiden. B&G has developed a technology, which successfully predicts whether mass violence attacks may occur in any member state of the EU. For this purpose, the technology uses personal data of all the citizens of the city of Amsterdam.

- a) Does the GDPR or Directive 2016/680 apply?
- b) Does B&G have to ask prior consent to the processing of the personal data?

<sup>31</sup> Article 5.1.e of the GDPR states that personal data should be kept no longer than necessary, but does not mention a number of days, months or years.

<sup>32</sup> WP29 (2017) Opinion WP 2017/258 on some key issues of the Law Enforcement Directive (EU 2016/680). Adopted 20 November 2017.



Law enforcement authorities may want to use profiling techniques for criminal investigation purposes or evidence gathering, but this is strictly regulated in Article 11 of the Directive.<sup>33</sup> It is not prohibited, but should be regulated by law, with appropriate safeguards and guarantees for the right to obtain human intervention. Similarly, the use of special categories of (sensitive) personal data, such as regarding ethnicity, sexual orientation and religious or political convictions, is restricted.

---

<sup>33</sup> It has been argued that the principles discussed in this chapter are incompatible with development in the area of big data, see Zarsky, T. (2017) Incompatible: The GDPR in the Age of Big Data. *Seton Hall Law Review*, Vol. 47, No. 4(2), 2017. See also WP29 (2017) Opinion WP 2017/258 on some key issues of the Law Enforcement Directive (EU 2016/680). Adopted 20 November 2017.



## Chapter 5: Data subject rights and data controller obligations

### 5.1 Data subject rights

Both the GDPR and Directive 2016/680 include a list of data subject rights, including a right to information and a right to access.<sup>34</sup> Table 5.1 provides an overview of the data subject rights in both legal instruments. From this overview it becomes apparent that the number of data subject rights in the GDPR is more extensive. Also, the data subject rights in Directive 2016/680 can be further restricted. At the same time, the collecting and processing of data by law enforcement authorities requires (special) investigation powers and the use of specific technologies.<sup>35</sup> Particularly online investigation powers may yield large amounts of (sometimes highly sensitive) personal data.<sup>36</sup>

Member States are explicitly granted the opportunity to create restrictions if necessary to avoid obstructing official or legal inquiries, investigations or procedures; avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties; protect public security; protect national security; or protect the rights and freedoms of others. These restriction may apply to all data subject rights, i.e., the right to information, the right to access, the right to rectification and the right to erasure.

The right to rectification applies to incorrect or incomplete data. The right to have personal data erased ('right to be forgotten') does exist in the Directive (art. 16), but is limited: instead of erasure, the data controller shall restrict processing where the accuracy of the personal data is contested but cannot be ascertained or when the personal data must be maintained for the purposes of evidence. The right to restriction of processing, the right to data portability and the right to object to automated individual decision-making do not exist in the Directive.

---

<sup>34</sup> WP29 (2017) Opinion WP 2017/258 on some key issues of the Law Enforcement Directive (EU 2016/680). Adopted 20 November 2017.

<sup>35</sup> For an overview of technologies used in law enforcement, see Custers, B., Vergouw, B. (2015) Promising policing technologies: Experiences, obstacles and police needs regarding law enforcement technologies, *Computer Law & Security Review*, 31, p. 518-526; Custers, B.H.M. (2012) Technology in Policing: Experiences, Obstacles and Police Needs, *Computer Law & Security Review*. Vol. 28, No. 1, p. 62-68.

<sup>36</sup> Oerlemans, J.J. (2017) *Investigating Cybercrime*, PhD thesis. eLaw - Center for Law and Digital Technologies, Meijer series no. MI-275. Leiden University.





Article 11 of the Directive, which is mentioned in a different Chapter of the Directive and hence may not typically be considered as a data subject right, mentions that automated processing, including profiling, is prohibited unless authorized by either the EU or national legislation. Similar to Article 22 of the GDPR, it does restrict data processing and is intended to further protect data subjects.<sup>37</sup> This restrictions in the Directive could be considered as a balance for the fact that data subjects cannot always be granted full data subject rights, such as the right to information, access and rectification.

Data subject right	Directive 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	N/A	Art. 18
Right to data portability	N/A	Art. 20
Right to object to automated individual decision-making	N/A	Art. 21-22

Table 5.1 *Overview of data subject rights in Directive 2016/680 vs the GDPR.*

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

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

<sup>37</sup> Custers B.H.M. (2013), Data Dilemmas in the Information Society. In: Custers B.H.M., Calders T., Schermer B., Zarsky T. (red.) *Discrimination and Privacy in the Information Society*. nr. 3 Heidelberg: Springer. 3-26.





illegally obtained (for instance, because a warrant is missing). Such sanctions may be, for instance, excluding such illegally obtained evidence, lowering the final sentences imposed or concluding that the entire case is not admissible to the court.

## 5.2 Data controller obligations

For data controllers a list of obligations with regard to the processing of personal data is included in both Directive 2016/680 and the GDPR. Table 5.2 provides an overview. These data controller obligations are to a large extent similar and address data protection by design and by default, maintaining records of the data processing activities, mandatory cooperation with the Data Protection Authorities (DPAs), performing data protection impact assessments, ensuring security of the processing of personal data, mandatory notifications to supervisory authorities and/or data subjects in case of data breaches, prior consultation with the DPA in case of high risks and designating data protection officers. For logging of processing operations there exists a special provision on Article 25 of the Directive. The implementation of logs is a crucial tool for data protection monitoring, hence for controlling all relevant data processing operations. In order to do so, it should be possible to trace user activity to spot abusive use. National laws should further develop the requirements for logging: on content, on storage periods, on technical measures, on self-auditing and on internal policies to promote compliance.<sup>38</sup> Data protection officers must be involved in the definition of the procedure in order to effectively delete or erase the data once the time limits for the storage have expired.<sup>39</sup>

All competent authorities should designate a data protection officer (DPO) according to article 32. However, member states can opt to exempt courts and other independent judicial authorities from the obligation to designate a data protection officer. The GDPR encourages the use of codes of conduct (art. 40-4 GDPR) and certification (art. 42-43 GDPR), but the Directive does not contain similar provisions.

---

<sup>38</sup> WP29 (2017) Opinion WP 2017/258 on some key issues of the Law Enforcement Directive (EU 2016/680). Adopted 20 November 2017.

<sup>39</sup> WP29 (2017) Opinion WP 2017/258 on some key issues of the Law Enforcement Directive (EU 2016/680). Adopted 20 November 2017.



Data controller obligation	Directive 2016/680	GDPR
Data protection by design	Art. 20	Art. 25
Data protection by default	Art. 20	Art. 25
Maintain records	Art. 24	Art. 30
Logging	Art. 25	N/A
Cooperation with the DPA	Art. 26	Art. 31
Data protection impact assessment	Art. 27	Art. 35
Security of processing	Art. 29	Art. 32
Data breach notification	Art. 30-31	Art. 33-34
Prior consultation with the DPA	Art. 28	Art. 36
Data protection officers	Art. 32-34	Art. 37-39

Table 5.2 *Overview of data controller obligations in Directive 2016/680 vs the GDPR.*

It is important to note that the data controller obligations also apply to data processors. Data controllers and data processors are not always the same entities. The data controller is the competent authority which, alone or jointly with others, determines the purposes and means of the processing of personal data (art. 3.8). The data processor means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller (art. 3.9). When data processors violate provisions in the Directive, they can be held accountable for this, but the data controller can also be held accountable. For instance, when a court outsources the structuring and analysis of its court files to a technological company, the court remains the data controller, but the technological company is a data processor. When the technological company (the data processor) is confronted with a data breach, the court (the data controller) can be held responsible and liable. Whether the technological company is also responsible and liable depends on the nature of the data breach and the exact circumstances.<sup>40</sup>

<sup>40</sup> For a further discussion on data breach notification laws, see for instance, Schneier, B. (2009) State Data Breach Notification Laws: Have They Helped? *Information Security*, January 2009.



**Example: minor offenses**

The company B&G B.V. is an Intelligence software company operating in the EU with HQ in Leiden. B&G has developed a technology, which identifies and prevents criminal organizations from operating within the EU. Once they have identified a potential criminal, member of a criminal organization, they inform the local authorities. For the identification process they use the data of people who conducted minor offences, like non-payments for train tickets. Are they eligible to do so?



## Chapter 6: Data transfers

One of the main goals of Directive 2016/680 is the protection of personal data of data subjects. Since many countries outside the EU are not offering such protection in their legal systems, there are strict rules in the Directive (and similarly in the GDPR) for the transfer of personal data to recipients outside the EU.<sup>41</sup> The transfer of personal data to third countries (i.e., all countries that are not EU member states) and international organizations is, in principle, prohibited. However, exceptions apply. Personal data in criminal law may be transferred outside the EU only to competent authorities and only when there is sufficient legal protection for data subjects in the receiving jurisdiction. Such protection can be based on an adequacy decision (art. 36), appropriate safeguards (art. 37), which will be explained below. When such protection is absent, transfer of personal data outside the EU may still take place in very specific situations (art. 38-39), for instance, in case of immediate and serious threats to public security.

Adequacy decisions are taken by the European Commission. When the receiving country or international organization has ensured (according to the commission) an adequate level of protection, data transfers do not require any further, specific authorization. Note that the level of protection must be adequate, which does not necessarily mean it has to be the same as within the EU. The adequacy decision depends on factors like the rule of law, respect for human rights and fundamental freedoms, relevant legislation, sectoral legislation, etc. According to the Schrems case, in which third country data transfers to the United States were contested, it became apparent that of particular importance are the Safe Harbour Treaty for data transfers between the EU and the US provided insufficient protection for data subjects.<sup>42</sup> The EU Court of Justice considered that due to the absence of the rights to access, rectification and erasure and the absence of the right to legal remedy adequate protection was not offered for data subjects. As a result, the court declared the Safe Harbour Treaty invalid.

When a country or international organization has not received a favourable adequacy decision, appropriate safeguards can be a legal basis to allow the transfer of personal data. Appropriate safeguards have to be provided for in legally binding instruments. These documents have to be approved by the Data Protection Authority. Again, data subject rights (such as the right to access, rectification and erasure) and the right to a legal remedy are important factors for obtaining approval.

---

<sup>41</sup> Bamberger, K.A. and Mulligan, D.K. (2015) *Privacy on the Ground: Driving Corporate Behavior in the United States and Europe*. The MIT Press.

<sup>42</sup> Judgment - 06/10/2015 – Schrems. Case C-362/14.



In case of an intended data transfer without an adequacy decision or appropriate safeguards, exceptions in art. 38 of Directive 2016/680 may apply for specific situations. Such data transfers may be allowed, for instance, when necessary to protect vital or legitimate interests of people, to prevent immediate and serious threats to public security. When cooperating with countries outside the EU, law enforcement authorities in the EU are allowed to directly request information from companies and citizens in a third country and they may include personal data in such requests (usually a name or an IP address).<sup>43</sup> Article 39 of the Directive contains further provisions for direct transfers of personal data Article 35.1.b to recipients that are not competent authorities.

Since criminals may want to reside in countries outside the EU that have little or none cooperation in the area of criminal investigation, the European Commission intends to promote the possibility of adequacy decisions with qualifying third countries, in particular with those countries with which close and swift cooperation is required in the fight against crime and terrorism, and where significant personal data exchanges are already taking place.<sup>44</sup> The 2016 agreement between the EU and the US on the protection of personal data in criminal law cooperation is an example of such cooperation in law enforcement with third countries.<sup>45</sup>

The rules for data transfers are highly relevant for the judiciary when examining cases in which personal data are transferred between countries. When personal data is transferred to third countries without a proper legal basis, this may cause harm to data subjects. Note that the Directive does not impose a lot of conditions on personal data that EU authorities receive from competent authorities outside the EU. Hence, the Directive focuses on personal data flows within the EU and on personal data leaving the EU, but not on personal data coming into the EU.

---

<sup>43</sup> See art. 39 and recital 73 of the Directive.

<sup>44</sup> COM(2017) 7 final, Exchanging and Protecting Personal Data in a Globalised World, Brussel, 10.1.2017.

<sup>45</sup> Agreement between the United States of America and the European Union on the protection of personal information relating to the prevention, investigation, detection, and prosecution of criminal offenses:

[http://ec.europa.eu/justice/data-protection/files/dp-umbrella-agreement\\_en.pdf](http://ec.europa.eu/justice/data-protection/files/dp-umbrella-agreement_en.pdf).



## Chapter 7: Supervision, cooperation and liability

### 7.1 Independent supervision and cooperation

On the basis of Directive 2016/680 every EU Member State has to establish a supervisory authority. This authority has to be completely independent and its competences, tasks and powers are described in articles 45, 46 and 47 respectively. Since there is a large amount of overlap, it is likely that the supervisory authority for the GDPR (the Data Protection Authority) is also the supervisory authority for Directive 2016/680. The Directive allows for this option, but member states are also allowed to establish a separate authority.

The most important element of these provisions for the judiciary can be found in Article 45.2 of the Directive. In this provision, the courts are excluded from the supervision of national Data Protection Authorities. In other words, national Data Protection Authorities are not competent for the supervision of data processing of courts when acting in their judicial capacity. Furthermore, Member States may provide for their national Data Protection Authorities not to be competent to supervise data processing of other independent judicial authorities when acting in their judicial capacity. Since Article 8.3 of the Charter of Fundamental Rights of the EU<sup>46</sup> requires that compliance with the fundamental right of protection of personal data shall be subject to control by an independent authority, another way of supervision must be envisaged in these cases. The exception for the judiciary in Article 45.2 of the Directive sees to the independent position of the judiciary. From the perspective of the separation of powers, it is important that there is no supervision on the judiciary that may influence their decision-making processes in court cases.<sup>47</sup>

As mentioned in Chapter 1, some Member States do not yet have any legislation in the field of personal data in criminal law, which means they have to establish a new authority or assign new tasks (and resources) to the data protection authority. In other countries, in which legislation already exists, it is likely that the incumbent supervisory authorities take over the supervision of Directive 2016/680.

International cooperation between law enforcement agencies and public prosecution services is crucial for any successes in the criminal investigation and prosecution of crime and terrorism, particularly in the area of cybercrime. For this reason, Directive 2016/680 also provides rules for international

---

<sup>46</sup> Charter of Fundamental Rights of the EU, 2000C 364/01.

<sup>47</sup> This exception does not apply to public prosecution services. Although public prosecution services generally have a high level of independence in many EU member states, their personal data processing can be supervised by the DPAs.



cooperation between supervisory authorities. In principle, supervisory authorities are obliged to help each other when information is requested. At the European level, supervision is further organized via the European Data Protection Board. This board is established via art. 68 GDPR and is a body of the EU and has legal personality. The board is composed of the head of one supervisory authority of each Member State and of the European Data Protection Supervisor, or their respective representatives.

## 7.2 Remedies, liability and penalties

Directive 2016/680 offers several legal remedies, including the right to lodge a complaint with a supervisory authority (art. 52), the right to an effective judicial remedy against a supervisory authority (art. 53), the right to an effective judicial remedy against a data controller or processor (art. 54), the right to be represented (art. 55) and the right to compensation (art. 56). The right to compensation concerns any material or non-material damage suffered by persons as a result of unlawful processing of personal data or any act infringing the national implementation laws of the Directive. Member states have to implement this in national law and can choose who can assign any compensations to data subjects, such as Data Protection Authorities, courts, ministries, etc.

The Directive also mandates Member States to lay down rules in national law on the penalties applicable to violations of the provisions adopted pursuant to the Directive (art 57). Any (maximum) amounts of compensation or fines are not mentioned in the Directive. Penalties should be effective, proportionate and dissuasive. The Directive does not contain any provision on administrative fines like Article 83 of the GDPR.

According to article 63 of the Directive, the deadline for the implementation of the Directive into national laws of member states is 6 May 2018. It is beyond the scope of this report to provide a complete overview of the implementation status in each member state. For instance, in the Netherlands, no draft legislation was yet proposed by the government. In Greece, a legislative law committee was established immediately after the GDPR and Directive 2016/680 were published. However, this committee had not completed its work by its deadline in May 2017 and was granted extension of the deadline until December 2017. Other countries made more progress. For instance, in the Czech Republic, a new data protection act that also implements Directive 2016/680 was published by the government in August 2017 and entered the legislative procedure. In Austria, the legislator put in force the national Data Protection Amendment Act 2018 (Datenschutz-Anpassungsgesetz 2018) in



June 2017. This act implements Directive 2016/680 in a separate chapter.<sup>48</sup> In Germany, the Act to adapt data protection law to Regulation (EU) 2016/679 and to implement Directive (EU) 2016/680 (DSAnpUG-EU) of June 2017 was adopted by the Bundestag with the approval of the Bundesrat.<sup>49</sup>

---

<sup>48</sup> <https://www.lw.com/admin/Upload/Documents/FINAL-GDPR-Implementation-Tracker.pdf>

<sup>49</sup> [https://iapp.org/media/pdf/resource\\_center/Eng-trans-Germany-DPL.pdf](https://iapp.org/media/pdf/resource_center/Eng-trans-Germany-DPL.pdf)





## Chapter 8: Conclusions

When reviewing Directive 2016/680 it is apparent that there is a lot of overlap with the GDPR, but there are also a number of noticeable differences. In short, Directive 2016/680 aims to set more specific rules for the processing in personal data in criminal law, since the GDPR does not always provide sufficiently adequate and detailed rules for the context of criminal law. Directive 2016/680 tries to provide a more contextualised balance. At the same time, on a more general level, this Directive constitutes a further harmonisation of criminal law across EU member states, facilitating the cooperation within the EU in the area of criminal law.

The goal of this report is to review Directive 2016/680 specifically for the judiciary, one of the target groups of the Directive. However, it has become apparent that there is almost no special provision for the judiciary within the Directive. One noticeable exception is that member states, when implementing the Directive in national law, can choose to exempt courts from specific obligations, such as the obligation to assign a data protection officer.

The fact that the judiciary is not specifically addressed as a separate target group in the Directive does not diminish the relevance of the Directive for the judiciary. On the contrary, the Directive is highly relevant for both roles of the judiciary, as the judiciary is processing (sometimes highly sensitive) personal data that are highly relevant in the prosecution and sentencing of crimes (both as clues in criminal investigation and as evidence in courts) and, as such, should be treated according to the rules, ensuring that all rights of suspects and other data subjects that may be involved in criminal law cases (such as witnesses, victims, etc.) are adequately protected.



## Bibliography

Bamberger, K.A. and Mulligan, D.K. (2015) *Privacy on the Ground: Driving Corporate Behavior in the United States and Europe*. The MIT Press.

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

Custers B.H.M. & Prinsen M.M. (2010), *Introduction to Forensics*. In: Herzog-Evans M (red.) *Transnational Criminology Manual*. Tilburg: Wolf Legal Publishers. 15-34.

Custers, B.H.M. (2012) Technology in Policing: Experiences, Obstacles and Police Needs, *Computer Law & Security Review*. Vol. 28, No. 1, p. 62-68.

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;

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>

R. Gellman (2012) Fair Information Practices: A Basic History, available at <http://bobgellman.com/rg-docs/rg-FIPShistory.pdf>.

Gonzales Fuster, G. (2014) *The Emergence of Personal Data Protection as a Fundamental Right of the EU*. Heidelberg: Springer, p. 220.



Hornung G. (2012) A General Data Protection Regulation for Europe? Light and Shade in the Commission" s Draft of 25 January 2012, 9 *SCRIPTed* 64-81.

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*.

Oerlemans, J.J. (2017) *Investigating Cybercrime*, PhD thesis. eLaw - Center for Law and Digital Technologies, Meijer series no. MI-275. Leiden University.

Ohm, P. (2010) Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization. *UCLA Law Review* 57, 1701–1765.

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.

Schneier, B. (2009) State Data Breach Notification Laws: Have They Helped? *Information Security*, January 2009.

Weisburd, D. and Telep, C.W. (2014) Hot Spots Policing: What We Know and What We Need to Know, *Journal of Contemporary Criminal Justice* 2014 30: 200.

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



WP29 (2018) Guidelines on Personal data breach notification under Regulation 2016/679. Article 29 Working Party, 6 February 2018.

WP29 (2018) Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679. Article 29 Working Party, 6 February 2018.

Wright, D., en Hert, P. de (2012), *Privacy Impact Assessment*, Heidelberg: Springer.

Zarsky, T. (2017) Incompatible: The GDPR in the Age of Big Data. *Seton Hall Law Review*, Vol. 47, No. 4(2), 2017.



## Appendix A: List of training authorities for the judiciary

Country	Training authority	Website
Austria	Federal Ministry of Justice – Department of Judicial Training	email: <a href="mailto:team.v@bmi.gv.at">team.v@bmi.gv.at</a> <sup>50</sup>
Belgium	Institute de Formation Judiciaire	<a href="http://www.igo-ifj.be">http://www.igo-ifj.be</a>
Bulgaria	National Institute of justice	<a href="http://www.nij.bg">www.nij.bg</a>
Croatia	Judicial Academy	<a href="http://www.pak.hr">www.pak.hr</a>
Cyprus	Supreme Court of Cyprus <sup>51</sup>	<a href="http://www.supremecourt.gov.cy">http://www.supremecourt.gov.cy</a>
Czech Republic	Judicial Academy	<a href="http://www.jacz.cz/">http://www.jacz.cz/</a>
Denmark	Court Administration – Domstolsstyrelsen	<a href="http://www.domstol.dk">http://www.domstol.dk</a>
Estonia	Supreme Court of Estonia – Training Department	<a href="http://www.riigikohus.ee">http://www.riigikohus.ee</a>
Finland	Ministry of Justice - Oikeusministerio	<a href="http://www.oikeusministerio.fi">http://www.oikeusministerio.fi</a>
France	Ecole Nationale de la Magistrature	<a href="http://www.enm.justice.fr">http://www.enm.justice.fr</a>
Germany	Deutsche Richterakademie	<a href="http://www.deutsche-richterakademie.de">www.deutsche-richterakademie.de</a>
Greece	ESDI - Εθνική Σχολή Δικαστικών Λειτουργών	<a href="http://www.esdi.gr/nex/index.php/el/">http://www.esdi.gr/nex/index.php/el/</a>
Hungary	Hungarian Academy of Justice - Magyar Igazságügyi Akadémia	<a href="http://mia.birosag.hu">http://mia.birosag.hu</a>
Ireland	Committee for Judicial Studies	<a href="http://www.courts.ie">http://www.courts.ie</a>
Italy	Scuola Superiore della Magistratura	<a href="http://www.scuolamagistratura.it">www.scuolamagistratura.it</a>
Latvia	Latvian Judicial Training Centre	<a href="http://www.ltmc.lv">http://www.ltmc.lv</a>
Lithuania	National Courts Administration	<a href="http://www.teismai.lt">www.teismai.lt</a>

<sup>50</sup> No website according to our research.

<sup>51</sup> According to research a specific training body in accordance with the EU standards will begin operating by January 2018 (<http://www.reporter.com.cy/local-news/article/225861/>).



Luxembourg	Parquet General	<a href="http://www.justice.public.lu/fr/organisation-justice/ministere-public/parquet-general/index.html">http://www.justice.public.lu/fr/organisation-justice/ministere-public/parquet-general/index.html</a>
Malta	Judicial Studies Committee	<a href="http://www.judiciarymalta.gov.mt/judicial_studies_committee">http://www.judiciarymalta.gov.mt/judicial_studies_committee</a>
Netherlands	Studiecentrum Rechtspleging	<a href="https://ssr.nl/">https://ssr.nl/</a>
Poland	National School of Judiciary and Public Prosecution	<a href="http://www.kssip.gov.pl">www.kssip.gov.pl</a>
Portugal	Centro dos Estudos Judiciarios	<a href="http://www.cej.mj.pt">http://www.cej.mj.pt</a>
Romania	Institutul National Al Magistraturii	<a href="http://www.inm-lex.ro">http://www.inm-lex.ro</a>
Slovakia	Justicna Akademia Slovenskej Republiky	<a href="http://www.ja-sr.sk">www.ja-sr.sk</a>
Slovenia	Ministry of Justice of the Republic of Slovenia – Judicial Training Centre	<a href="http://www.mp.gov.si/en/judicial_training_centre/">http://www.mp.gov.si/en/judicial_training_centre/</a>
Spain	Centro De Estudios Juridicos	<a href="http://www.cej-mjusticia.es">http://www.cej-mjusticia.es</a>
Sweden	Courts of Sweden Judicial Training Academy	<a href="http://www.domstol.se">http://www.domstol.se</a>
United Kingdom	Judicial College	<a href="http://www.judiciary.gov.uk/">http://www.judiciary.gov.uk/</a>

