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

Lauri J. Pajunoja

Master´s thesis
University of Helsinki
Faculty of law
The Erik Castrén Institute of International Law and Human Rights
Public international law
Supervised by Sahib Singh & Samuli Miettinen
2017

Tiedekunta/Osasto - Fakultet/Sektion – Faculty	Laitos - Institution – Department
Faculty of law	The Erik Castrén Institute of International Law and Human Rights

Tekijä - Författare – Author

Lauri Johannes Pajunoja

Työn nimi - Arbetets titel – Title

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

Oppiaine - Läroämne – Subject

Public international law

Työn laji - Arbetets art – Level	Aika - Datum – Month and year	Sivumäärä - Sidoantal – Number of pages
Master´s thesis	March 2017	96

Tiivistelmä - Referat – Abstract

The EU´s data protection law is under reform. The Union has adopted the General Data Protection Regulation 2016/679[1] (GDPR) to repeal the Data Protection Directive 95/46/EC[2] (DPD), which is currently governing the protection of personal data in EU. The Data Protection Directive does not apply to activities in the areas of judicial cooperation in criminal matters and police cooperation. To fix this lack of scope the EU adopted the Data Protection Directive on Police Matters 2016/680[3]. These adopted legislative instruments will step in force at May 2018.

The question of this thesis is whether the Data Protection Directive on Police Matters ensures protection of the right to privacy. This new Directive aims to ensure that natural persons´ level of protection of the rights and freedoms is equivalent in all member states in relation to the processing of their personal data in police matters.[4] The Directive harmonizes the legislation in minimum level. It allows the member states to adopt stronger protection and stricter provisions on data protection.

This thesis answers to the question with three points. Firstly, with optimistic interpretation that it does as in the legislative level the protection is already good. Union´s already existing data protection principles are just going to be extended to cover the field of police matters. Secondly, with realistic approach that it is too early to say. The member states legislative traditions differ from each other and the forthcoming Directive is abstract. It leaves member states room to interpret it, and the implementation is not yet ready. And thirdly, the implementation of the new Directive has problems because the member states´ national systems and the cultures of application differ. Some countries, like Finland, have dozens of manuals and handbooks of data protection principles to be applied in practice and even compulsory online courses to be passed by the officers in order to be allowed to practice their profession. Some member states do not have such procedures and the cultures of judicial cooperation are not at the same level between countries.

The authorities try to fight against serious crimes and terrorism and in that fight they occasionally interfere with individuals' fundamental rights. They must balance between two interests: the maintenance of national security and the maintenance of adequate protection of personal data and privacy. These interests should not be seen as competing interests in sense that if the other is well protected the other would not be protected. The developing technology enables new and more extensive possibilities for authorities to interfere with individuals´ fundamental rights. The legislators should keep this in mind when evaluating needs to develop new rules to guide the interfering measures.

Avainsanat – Nyckelord – Keywords

International law, data protection, privacy

Säilytyspaikka – Förvaringställe – Where deposited

Faculty of law at the University of Helsinki

Muita tietoja – Övriga uppgifter – Additional information

[1] EU Regulation 2016/679, General Data Protection Regulation.
[2] EU Data Protection Directive 95/46/EC.
[3] EU Data Protection Directive on Police Matters 2016/680.
[4] Ibid, Recital 7.

TABLE OF CONTENTS

LIST OF ABBREVIATIONS

Charter	Charter of Fundamental Rights of the EU
CIS	Customs Information System
CJEU	Court of Justice of the European Union
CoE	Council of Europe
DPD	Data Protection Directive 95/46/EC
ECtHR	European Court of Human Rights
ECHR	European Convention on Human Rights
EDPB	European Data Protection Board
EDPS	European Data Protection Supervisor
Eurosur	European Border Surveillance System
GDPR	General Data Protection Regulation 2016/679
ISP	Internet Service Provider
NSA	National Security Agency
OECD	Organisation for Economic Co-operation and Development
SIS	Schengen Information System
TEU	Treaty on European Union
TFEU	Treaty on the Functioning of the European Union
VIS	Visa Information System

DEFINITIONS[5]

Data subject	Natural person
Personal data	Information relating to an identified or identifiable natural person.
Profiling	Any form of automated processing of personal data consisting of the use of personal data to evaluate personal aspects relating to a natural person, in particular to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements
Pseudonymisation	The processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.
Competent authority	Any public authority, body or entity entrusted by Member State law to exercise public powers and 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
Controller	EU law: Who "*alone or jointly with others determines the purposes and means of the processing of personal data*". CoE law adds that a controller decides which categories of personal data should be stored.
Processor	A natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.
Processing	Any operation which is performed upon personal data, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.
Genetic data	Personal data, relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health

[5] EU Data Protection Directive 95/46/EC, Article 2; EU Data Protection Directive on Police Matters 2016/680, Article 3; Convention 108, 1981, Article 2.

	of that natural person and which result from an analysis of a biological sample from the natural person in question
Biometric data	Personal data resulting from specific technical processing relating to the physical, physiological or behavioral characteristics of a natural person, which allow or confirm the unique identification of that natural person
Supervisory authority	An independent public authority which is established by a Member State pursuant to Article 41
Third party	A natural or legal person, public authority, agency or any other body other than the data subject, the controller, the processor and the persons who, under the direct authority of the controller or the processor, are authorized to process the data.
Recipient	A natural or legal person, public authority, agency or any other body to whom data are disclosed. Authorities which may receive data in the framework of a particular inquiry are not regarded as recipients
Data subject´s consent	Freely given specific and informed indication of her wishes by which the data subject signifies her agreement to personal data relating to her being processed.

INTRODUCTION

The objective of the thesis

The Finnish Police Code defines the duty and mission of law enforcement agencies, whose task is the protection of legal and judicial order in society, the maintenance of public order and security, as well as general crime prevention, investigation and placing to prosecution. As such, the police are tasked with cooperating with other officials, residents, and society as a whole in order to maintain public security, in addition to taking care of international cooperation in this field.[6]

This research introduces the duty of law enforcement agencies concerning the protection and exchange of personal data between the EU member states´ investigative authorities, namely the police. The authorities try to fight against serious crimes and terrorism and in that fight they occasionally interfere with individuals' fundamental rights. The authorities must maintain a balance between two interests: the maintenance of national security and the adequate protection of personal data and privacy. These interests should not be seen as competing in the sense that if the other is well protected the other would not be protected.

The EU´s data protection law is currently under reform. The Union has adopted the General Data Protection Regulation[7] (GDPR) to repeal the Data Protection Directive 95/46/EC[8] (DPD), which is currently governing the protection of personal data in the EU. The DPD applies to processing of personal data in member states in the public and the private sectors, but it does not apply to activities in the areas of judicial cooperation in criminal matters and police cooperation. To fix this lack of scope, the EU adopted the Data Protection Directive on Police Matters 2016/680[9].

The core question of this thesis is whether the Data Protection Directive on Police Matters ensures the protection of the right to privacy. It will be answered with three points. Firstly, with an optimistic interpretation espousing that it does as the legislative level of protection is already good and the data protection principles are just going to be extended to cover

[6] Poliisilaki 872/2011, Section 1(1).
[7] EU Regulation 2016/679, General Data Protection Regulation.
[8] EU Data Protection Directive 95/46/EC.
[9] EU Data Protection Directive on Police Matters 2016/680.

police matters. Secondly, with the realistic approach. It is currently too early to say as the Directive is just being implemented. And thirdly by presenting threats to the Directive´s implementation. The member states´ legislations and cultures differ from each other as well as the new Directive´s abstract provisions gives the member states room for interpretation.

The structure of the thesis

This thesis asks whether the forthcoming legal instrument will ensure the protection of privacy in the EU. On many occasions, the thesis will discuss the concept of adequate protection of privacy. The "adequacy" will not be put forth as such as there is currently no EU level standard for it, except when personal data is sent from an EU state to a third country. Adequacy of protection is an evolving concept. The level of protection of personal data and the protection of privacy must be evaluated on a case-by-case basis. This evaluation considers the whole chain of actions conducted in the processing of personal data and continues through the entire lifespan of the data. There is no such magical article from which protection can be invoked. Therefore, this paper will go through all the relevant legislation governing the field and introduce the evolution of the data protection principles in relation to privacy in the case law European Courts.

This paper is divided into four sections. The first section introduces the current European legislation covering the investigative authorities´ work in relation to the protection of personal data and the protection of the right to privacy. It explains the operation of both systems, those being the legislations of the Council of Europe (CoE) and the EU and after this it shows the main principles guiding the processing of personal data. The second section goes through the recent trends found in the European Courts in relation to the protection of personal data and privacy. The second section first scans the principles and interpretations laid down by the European Court of Human Rights (ECtHR) and then the Court of Justice of the European Union (CJEU). Via those cases, this thesis shows the connection between the European Convention on Human Rights (ECHR) and the Charter of Fundamental Rights of the European Union (Charter) as well as the CJEU´s link to the interpretations of the ECtHR.

The third section will explain how the EU´s legislation on data protection is going to change in the field of police matters. The forthcoming Data Protection Directive on Police Matters sets new guidelines for the member states to protect personal data in criminal matters. It is a Directive "*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*"[10]. The third section introduces the aspects which effected on the growing need for uniformed data protection in this field and the phases of the data protection reform.

The fourth section states that the forthcoming Data Protection Directive on Police Matters does protect the right to privacy, and it answers to this core claim of the thesis. This section introduces the current Finnish data protection practices in the public authorities´ work as possible examples for other EU states on how they could adapt their national systems. Lastly, the section introduces what problems the new Directive may face when it is being implemented into national legislations and what advantages the Union wide uniform data protection legislation brings with it.

Understanding the terms "privacy" and "data protection"

The term "privacy" may, in some countries mean the same thing or refer to the same principles as when other countries refer to "data protection". It may also be that in some countries the "data protection" is used to mean "information security" which may slightly overlap with "privacy". The term "data protection" may refer to the protection of personal information and the protection of confidential and valuable information, trade secrets, know-how, as well as similar information assets. So, the uses of the terms "data protection" and "privacy" differ based on where those are adopted, maybe because of the language spoken or depending on the region where the country is located. In the US, the term "privacy" seems to prevail when identifying the rules and practices in collection of data, use and processing of personal information, while outside the US, the term "data protection" has been more widely used than "privacy."[11]

[10] EU Data Protection Directive on Police Matters 2016/680.
[11] Gilbert, 2014.

Individuals usually want to have their human rights protected. Susanna Lindroos-Hovinheimo considers this to be a collective demand. When individuals want the state to protect their personal data and the right to privacy, this is a demand by an individual for herself. The demand is not for the collective. The society does not have a joint goal. Individuals have lost their ability to have an effect on their material, physical and economic conditions. The only thing they have left is the control of their private self-image. The lives lived and the lives narrated wind-up together and they both can be influenced by regulating the right to the protection of privacy and personal data.[12]

Public authorities collect and control information concerning persons, natural and legal. This term "information" consists of everything from personal identification numbers, home addresses and possessed vehicles to possible criminal records, health matters and so on. The public authority should be under surveillance and should operate according to the law concerning its maintenance of the person's information. This new Directive and this thesis both talk about "competent authorities" who handle personal data. These may include public authorities such as the judicial authorities, the police, and other law-enforcement authorities or anyone assigned by member state law to exercise public authority for this Directives´ purposes.[13]

Occasionally this thesis makes broad claims of public officials´ work in practice without fully justifying them. The reason for this is that the author is a public official while writing the paper and the information is classified in some cases.

[12] Lindroos-Hovinheimo, 2016, p. 133.
[13] EU Data Protection Directive on Police Matters 2016/680, Recital 11.

1 THE PROTECTION OF PRIVACY AND PERSONAL DATA IN THE EUROPEAN AUTHORITIES WORK TODAY

This first section of the paper will introduce the concepts of protecting personal data and privacy and the relevant legislations of the field in the Europe, dividing into the areas of the CoE and the EU. Approximately half of the CoE countries form the EU and the EU member states are under two different jurisprudences, the law of the CoE and the law of the EU. Even though this thesis is focused on data protection from the perspective of investigative authorities, it will nevertheless introduce the main legislative tools and data processing principles covering the field from the individual´s perspective as well.

1.1 CoE legislation related to the right to privacy and data protection

This chapter explains in detail how the individual´s rights to the protection of privacy and to the protection of personal data are regulated in the CoE´s legislation. The CoE was founded in 1949 and today it has 47 member states. The CoE can enforce international agreements agreed upon by European states.[14] The best-known body of the CoE is the ECtHR, which enforces the human rights instrument the ECHR.[15] Individuals, NGOs and legal persons can bring cases directly to the ECtHR,[16] which the CoE member states have implemented or given effect to in their national legislation so they must comply with it.[17]

The ECHR, written in 1949, does not contain provisions on protecting individual´s personal data and it does not mention "privacy". Instead it rules about the right to respect for private life which can be understood to mean the same thing. Article 8[18] states that:

1. "*Everyone has the right to respect for his private and family life, his home and his correspondence.*

[14] The Council of Europe in brief, Who we are, 2016.
[15] Neacşu, 2015. Chapter 4. European Union Agency for Fundamental Rights and Council of Europe, 2014, p. 14. Originally the ECHR established two judicial bodies: the European Commission of Human Rights alongside the ECtHR. The Commission operated, from 1953 until 1999 as an intermediary preventing trivial cases entering the ECtHR. UNHCR, Council of Europe: European Commission on Human Rights, 2016. Before 1998, natural persons did not have direct access to the ECtHR. First, they had to apply to the Commission, which would refer the case in the ECtHR on individual's behalf.
[16] ECHR Protocol No. 11 to the Convention for the Protection of Human Rights and Fundamental Freedoms, restructuring the control machinery established thereby, ETS No.155, 1998.
[17] ECHR, 1950, Article 19: "*To ensure the observance of the engagements undertaken by the High Contracting Parties in the Convention and the Protocols thereto, there shall be set up a European Court of Human Rights, hereinafter referred to as "the Court". It shall function on a permanent basis*".
[18] Ibid, Article 8.

2. *There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others*"

The ECtHR is the only international court that has jurisprudence regarding the right to privacy.[19] It has clarified[20] that the ECHR Article 8 obliges states to refrain from actions which might violate this right and that the states are also under positive obligation to actively secure effective respect for privacy.[21]

1.1.1 The Convention 108 is the first data protection instrument

The CoE Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data (Convention 108)[22] is the first binding international instrument protecting individuals against abuses which may accompany the collection and processing of personal data. The Convention 108 applies to all data processing carried out by the private and public sectors, such as investigative authorities. It demands that the collected and processed data is adequate, relevant, proportionate and accurate. It is ratified by the CoE member states (currently 47), and it is also open to non-CoE states (as an example Senegal and Uruguay have ratified it[23]).[24] Formally Convention 108 has one purpose: to ensure data protection.[25] It also secures the free flow of data and has provisions on "trans-border data flows".[26] It prohibits restriction to flows of personal data going to another party´s territory taken "for the sole purpose of the protection of privacy"[27].

According to the Convention 108, data protection deals with the protection of natural persons, but the signatories can extend the protection also to legal persons in their national law.[28] The Convention provides guarantees in relation to the collection and processing of personal data and prohibits the processing of "sensitive" data on a person's race, politics, health, religion, sexual life, criminal record, etc., if appropriate legal safeguards are not in

[19] Cocq, 2016, p. 188.
[20] ECtHR, No. 20511/03, I. v. Finland, 17.7.2008. & ECtHR, No. 2872/02, K.U. v. Finland, 2.12.2008.
[21] European Union Agency for Fundamental Rights and Council of Europe, 2014, p. 15.
[22] Convention 108, 1981.
[23] Council of Europe, Treaty office, 2016.
[24] European Union Agency for Fundamental Rights and Council of Europe, 2014, p. 16-17.
[25] Convention 108, 1981, Article 1.
[26] Ibid, Chapter 3.
[27] Ibid, Article 12(2).
[28] European Union Agency for Fundamental Rights and Council of Europe, 2014, p. 38.

place. It enshrined individuals´ right to know what information is stored on them and to correct false information. The rights laid down in the Convention 108 may be restricted when overriding interests (such as state security, etc.) are at stake. The Convention provides restrictions on cross-border transmission of personal data to states where legal regulation does not provide equal and adequate protection.[29]

Convention 108 addresses the notion of quality of data, special categories of data and data security.[30] The notion of data quality is important as it refers to the idea that: [31]

- the personal data´s automatic processing must be fair and lawful;
- the data must be stored for specified and legitimate purposes and that data should not be used in a way incompatible with those purposes;
- the data must be adequate, relevant, and not excessive in relation to such purposes;
- the data must be accurate and kept up to date and kept in a form enabling the identification of the data subjects only if it is necessary.

In relation to the data subject´s rights the Convention recognizes: the right to information on the existence of automated personal data files and on the controller of the files; the right to access the stored data concerning her; the right to obtain rectification or erasure of the data if it is processed unduly; and the right to have a remedy in case of lack of compliance.[32] The Convention allows derogation from these principles if the measure is provided for by the national law and constitutes a necessary measure in a democratic society to protect state security, public safety, the state´s monetary interests or the prevention of criminal offences and protecting the rights and freedoms of others or the data subject.[33]

Convention 108 considers that the protection of personal data serves privacy. To justify the reference to the right to the protection of personal data, it has been argued that the right has acquired an autonomous meaning through the case law of the ECtHR. This is dealt in the section 2. Since 2011 Convention 108 has been under reconsideration.[34]

[29] Summary of Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 28.1.1981.
[30] Convention 108, 1981, Article 7.
[31] Ibid, Article 5(a) - (e).
[32] Ibid, Article 8(a) – (d).
[33] Ibid, Article 9.
[34] Fuster, 2014, p. 91.

1.1.2 The CoE legislation on data protection in police matters

Convention 108 covers data protection in police matters although the member states may limit its application.[35] The public authorities' tasks may require processing of an individual's personal data in a way which brings consequences to her. The CoE adopted the Police Data Recommendation[36] in 1987 to guide Convention 108 parties in the context of processing personal data by the national authorities. This Recommendation is not legally binding, but it guides on the collection of data for police work; who can access the data; what are the conditions for transferring data to foreign authorities; how the data subjects can exercise their data protection rights; and how to implement the independent authorities´ control. There is also an obligation to provide adequate data security.

Personal data should be collected only when needed to prevent a real danger or to suppress a specific criminal offence. Sensitive data´s processing is limited to what is necessary in the context of a specific inquiry. If personal data are collected without the data subject´s knowledge, she must be informed of the collection as soon as it does not disturb the investigations any longer. If police collect personal data by automated means, it should be based on specific provisions.[37] The retention of personal data by public authorities interferes with the ECHR Article 8(1). The stored administrative data should be distinct from the police data, as well as the data between different data subjects. The facts must be distinct from the suspicions.[38] The use of police data should be strictly limited to the purpose of collection. That data may be transferred within the police sector only if there is a legitimate interest for such exchange. It may be transferred outside the police sector only if there is a legal obligation or authorization for this. International transfer is restricted to foreign police authorities. It must be based on legal provisions and international agreements unless there is a necessity in preventing imminent danger.[39]

There must be a national independent authority to supervise the police´s data processing to make sure it complies with domestic data protection law. The data subjects are entitled to have all the access rights provided by Convention 108. If these rights are restricted under

[35] Convention 108, 1981, Article 3.
[36] CoE Police Data Recommendation Rec(87)15, 17.9.1987.
[37] Ibid, Principles 1 – 8.
[38] Ibid, Principle 3.
[39] Ibid, Principle 5.

Convention 108 Article 9[40] for the need of police investigations, the data subject must be able to appeal to the national data protection supervisory authority or to another independent body, which makes sure the refusal of access is well founded.[41]

The CoE has adopted the Convention on Cybercrime to handle the issue of crimes committed against and by means of electronic networks.[42] This Convention developed the protection of personal data and the authorities´ rights to cooperate internationally[43] as well as to search computer networks and to intercept individual´s communications[44]. This Convention requires parties to update and harmonize their criminal laws against hacking and other security infringements and illicit cyber-activities[45]. The signatories must protect human rights adequately, including the right to privacy.[46] The Convention has currently 49 ratifications, also the non-CoE members may accede to it.[47]

1.2 EU legislation related to the right to privacy and data protection

This chapter will go through how the rights to privacy and to the protection of personal data are regulated in the EU. The 28 EU member states must be able to rely on a high level and uniform data protection to enable the free flow of data which is required for the freedom of movement in the internal market[48]. The Union should act jointly to offer European citizens a high level of protection in the area of freedom, security and justice.[49]

[40] Convention 108, 1981, Article 9(2)(A): Derogation from the provisions of Convention Articles 5, 6 and 8 shall be allowed when such derogation is provided for by the law of the Party and constitutes a necessary measure in a democratic society in the interests of a protecting State security, public safety, the monetary interests of the State or the suppression of criminal offences.
[41] CoE Police Data Recommendation Rec(87)15, 17.9.1987, Principle 6.
[42] CoE Convention on Cybercrime CETS No. 185, 23.11.2001.
[43] Ibid, Chapter 3 provides general principles relating to international co-operation, to extradition, to mutual assistance, procedures pertaining to mutual assistance requests in the absence of applicable international agreements, and mutual assistance regarding investigative powers as well as 24/7 Network.
[44] Ibid, Articles 19 and 21.
[45] Ibid, Articles 7 - 10.
[46] Ibid, Preamble & Article 15(1): Each party ensures that the establishment, implementation and application of the powers and procedures are subject to domestic law´s safeguards, which provides for the adequate protection of human rights and liberties, including rights arising pursuant to obligations under the ECHR and other international human rights instruments, and which incorporates the proportionality principle.
[47] Full list, Chart of signatures and ratifications of Treaty 185, Convention on Cybercrime, Council of Europe, 2.10.2016. By October 2016 it was ratified, as non-CoE members, by Australia, Canada, Dominican Republic, Israel, Japan, Mauritius, Panama, Sri Lanka, and the United States. The only CoE states which have not signed the Convention are San Marino and Russia.
[48] TEU, Article 3(3): EU has established an internal market. (TFEU), Article 26: It is an area without internal borders to ensure the free movement of persons, capital, goods and services.
[49] TEU, Article 3(2): EU develops and maintains an area of freedom, security and justice without internal frontiers, where persons' freedom of movement is ensured in connection with adequate measures referring to external border controls, asylum, immigration and the prevention of crime.

This area establishes respect for fundamental rights and the different legal systems and traditions of the member states.[50] The topic of this thesis falls in the area of freedom, security and justice, which belongs into the third pillar of police and judicial cooperation in criminal matters[51]. In this field the Union and the member states have the shared competence to legislate.[52] The CJEU can hear preliminary matters under the third pillar as the courts last resort, and to hear references on the interpretation of, for example, framework decisions under it if the member states have accepted the Court's jurisdiction.[53]

1.2.1 EU´s primary law related to data protection and privacy

This chapter will introduce the main provisions related to the protection of personal data and the right to privacy in the EU today. The Lisbon Treaty[54], which came into force in 2009, modified the EU´s architecture for the protection of fundamental rights in general. It created the EU´s current human rights legislation as it amended the two treaties, the TEU[55] and the TFEU[56], and gave the Charter the same legal value as the treaties.[57]

The protection of personal data is regulated by TFEU Article 16, which states that[58]:

1. *Everyone has the right to the protection of personal data concerning them.*
2. *The European Parliament and the Council, acting in accordance with the ordinary legislative procedure, shall lay down the rules relating to the protection of individuals with regard to the processing of personal data by Union institutions, bodies, offices and agencies, and by the Member States when carrying out activities which fall within the scope of Union law, and the rules relating to the free movement of such data. Compliance with these rules shall be subject to the control of independent authorities. The rules adopted on the basis of this Article shall be without prejudice to the specific rules laid down in Article 39 of the Treaty on European Union.*

[50] Barnard, 2013, p. 12. TFEU, Article 67(1). In simple, the "freedom" refers to the absence of internal border controls for persons and a shared policy towards the third-country nationals. "Security" refers to the measures for preventing and fighting xenophobia, racism, and crime, but also to the cooperation between judicial authorities and other competent authorities as well as mutual recognition of judgements in criminal matters. The "justice" refers to the access to justice based on the principle of mutual recognition of judicial decisions in civil matter.
[51] TEU, Title VI.
[52] TFEU, Article 4, shared competence: both the EU and the member states may legislate, but member states only to the extent that the EU has not exercised its competence first (internal market, consumer protection, and the area of freedom, security and justice).
[53] Barnard, 2013, p. 542.
[54] Treaty of Lisbon amending the TEU and the Treaty establishing the European Community, 2007.
[55] TEU.
[56] TFEU.
[57] Fuster, 2014, p. 230-231.
[58] TFEU, Article 16.

Article 16(2) brings a new dimension to the EU arena by providing a legal basis for the Parliament and the Council to lay down rules on personal data for data processing falling under EU law. The TEU adds Article 39 which states[59] that:

> "*In accordance with [the TFEU] Article 16 and by way of derogation from paragraph 2 thereof, the Council shall adopt a decision laying down the rules relating to the protection of individuals with regard to the processing of personal data by the Member States when carrying out activities which fall within the scope of this Chapter, and the rules relating to the free movement of such data. Compliance with these rules shall be subject to the control of independent authorities*."

The Charter is a new treaty embodying the EU data protection law.[60] Originally it was not a legally binding document when it was ratified in 2000. In 2009 the Lisbon Treaty made it as part of the Union´s primary law.[61] The right to privacy is guaranteed in the Charter Article 7 which states that: "*everyone has the right to respect for his or her private and family life, home and communications.*"

The right to the protection of personal data is regulated in the Charter Article 8:

1. *Everyone has the right to the protection of personal data concerning him or her.*
2. *Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.*
3. *Compliance with these rules shall be subject to control by an independent authority.*

The Explanations of the Charter´s Articles states[62] that Article 8 is based on the Lisbon Treaty Article 286[63], which was then replaced by the TFEU Article 16[64], the TEU Article 39[65] and DPD[66], as well as on the ECHR Article 8[67] and on Convention 108[68]. The

[59] TEU, Article 39.
[60] European Union Agency for Fundamental Rights and Council of Europe, 2014, p. 20.
[61] Treaty of Lisbon amending the TEU and the Treaty establishing the European Community, 2007, Article 6(1): The Union recognizes the rights, freedoms and principles set out in the Charter, which shall have the same legal value as the Treaties.
[62] Explanations relating to the EU Charter, 14.12.2007, Explanation on Article 8.
[63] Treaty of Lisbon amending the TEU and the Treaty establishing the European Community, 2007, Article 286: "*1. From 1 January 1999, Community acts on the protection of individuals with regard to the processing of personal data and the free movement of such data shall apply to the institutions and bodies set up by, or on the basis of, this Treaty. 2. Before the date referred to in paragraph 1, the Council, acting in accordance with the procedure referred to in Article 251, shall establish an independent supervisory body responsible for monitoring the application of such Community acts to Community institutions and bodies and shall adopt any other relevant provisions as appropriate*."
[64] TFEU, Article 16: see footnote 58.
[65] TEU, Article 39: See footnote 59.

Explanations refers also to EU Regulation 45/2001[69] containing conditions and limitations for the exercise of the right to the personal data protection.[70] Article 8 was formed several years after the DPD so it can be considered as embodying the pre-existing EU data protection law. The Article´s second part refers to the key data protection principles and the third part provides that an independent authority should be established for controlling the implementation of these principles.[71] By recognizing the right to data protection, the Charter in fact created it.[72]

The Charter Article 52 sets the scope of rights guaranteed by the Charter and accepts limitations on their utilization. The limitations must be provided for by law and respect the essence of those rights and freedoms. The limitations must be necessary and proportionate. They must meet the general interest objectives recognized by the EU or to protect the rights and freedoms of others.[73]

The Charter strengthens the already existing rights instead of creating new ones, when it declares that the Charter confirms the fundamental rights guaranteed by the ECHR and as they result from the constitutional traditions common to the member states.[74] It has been described as an innovative instrument allowing the EU to follow the changes in society and

---

[66] EU Data Protection Directive 95/46/EC.
[67] ECHR, Article 8: see footnote 18.
[68] Convention 108, 1981.
[69] EU Regulation 45/2001, on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, 18.12.2000.
[70] Explanations relating to the EU Charter, 14.12.2007, Explanation on Article 8.
[71] European Union Agency for Fundamental Rights and Council of Europe, 2014, p. 20.
[72] Fuster, 2014, p. 2.
[73] Charter of fundamental rights of the EU, 2009, Article 52: "*1. Any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others. 2. Rights recognised by this Charter for which provision is made in the Treaties shall be exercised under the conditions and within the limits defined by those Treaties. 3. In so far as this Charter contains rights which correspond to rights guaranteed by the [ECHR], the meaning and scope of those rights shall be the same as those laid down by the said Convention. This provision shall not prevent Union law providing more extensive protection. 4. In so far as this Charter recognises fundamental rights as they result from the constitutional traditions common to the Member States, those rights shall be interpreted in harmony with those traditions. 5. The provisions of this Charter which contain principles may be implemented by legislative and executive acts taken by institutions, bodies, offices and agencies of the Union, and by acts of Member States when they are implementing Union law, in the exercise of their respective powers. They shall be judicially cognisable only in the interpretation of such acts and in the ruling on their legality. 6. Full account shall be taken of national laws and practices as specified in this Charter. 7. The explanations drawn up as a way of providing guidance in the interpretation of this Charter shall be given due regard by the courts of the Union and of the Member States."*
[74] EU Declaration No 1 concerning the Charter of Fundamental Rights of the European Union, annexed to the Final Act of the Intergovernmental Conference which adopted the Treaty of Lisbon, 13.12.2007.

technological developments.[75] It reaffirms the fundamental rights as they result from "*the constitutional traditions and international obligations common to the Member States*", as well as from the EU´s primary law, the ECHR, the Social Charters adopted by the Community and the CoE, and the case law of both the CJEU and the ECtHR.[76]

1.2.2 EU´s secondary law related to data protection

As the primary law of the rights to data protection and privacy is written in a few separate Articles in different Treaties, the secondary law is spread in several different instruments[77] covering specific issues. Since its adoption in 1995 the EU´s main legal instrument to protect personal data has been the DPD[78], which aimed to harmonize the data protection laws in the Union at the national level.[79] The object of the DPD is to ensure that the member states protect the fundamental rights and freedoms of natural persons and their right to privacy with respect to the processing of personal data. The free flow of personal data between the member states should not be restricted nor prohibited.[80]

The DPD gives substance to the principles of the right to privacy and data protection which were contained in Convention 108 and strengthens them.[81] The DPD does not apply in the areas of the processing of personal data by private individuals for personal purposes, nor to the matters outside of the internal market - the police and criminal justice cooperation.[82] But it does apply when a private person publishes data about others by using internet.[83]

[75] EU Commission, Communication from the Commission: Strategy for the effective implementation of the Charter of Fundamental Rights by the European Union. COM (2010) 573, 19.10.2010, p. 3.
[76] Charter of fundamental rights of the EU, 2009, Preamble.
[77] Rosas & Armati, 2012, p. 61–63, The secondary law are Regulations, Directives, Decisions, Opinions and Recommendations and Conventions, and international Agreements. And (TFEU), Article 288: Regulations are directly applicable to the member states and they bind in their entirety. Directives are binding upon each member state to which it is addressed, but they leave the choice of form and methods of how it is enforced to the national authorities. Decision is binding in its entirety or if it addresses its objects, it binds only on them. Recommendations and Opinions do not have binding force.
[78] EU Data Protection Directive 95/46/EC.
[79] What is an EU Directive?, 28.8.2016: Directive sets the objectives which must be reached Union widely. They are directed at the member states which then gives effect to its terms by passing domestic legislation. They may set minimum standards to be applied at national level, or allow member states to apply stricter national measures, if those do not conflict with the rules on free movement and free market.
[80] EU Data Protection Directive 95/46/EC, Article 1.
[81] Ibid, Recital 11.
[82] Ibid, Article 3(2).
[83] CJEU, C-101/01, Bodil Lindqvist, 6.11.2003, paras 27 & 47.

Additionally, to the DPD there is often a need for more detailed data protection provisions in different areas. The EU adopted the E-Privacy Directive 2002/58/EC[84] (on privacy in electronic communications), which established that member states may "*adopt legislative measures providing for the retention of data for a limited period*", for purposes such as security or crime prevention.[85] This enabled the member states to operate against the basic principle that traffic data must be erased or made anonymous as soon as possible. The Data Retention Directive 2006/24/EC[86] is to obligate telecommunication service providers to retain specified metadata for periods between 6 months and 2 years. This is to ensure the data's availability for the investigation and prosecution of serious crime. The main objective is to harmonize member states' law regarding data retention, which must comply with the Charter Articles 7 and 8.[87]

The Union lacked a data protection tool for the protection of individuals' privacy when the EU institutions processed their personal data, as the DPD addresses to the member states.[88] For this task the EU established the EU Institutions Data Protection Regulation 45/2001[89]. This Regulation is also important as it established the European Data Protection Supervisor (EDPS).[90] The EDPS is an independent body monitoring the application of the data protection rules by EU institutions and bodies, and it advices these institutions and the data subjects on matters concerning the processing of personal data. EU citizens can complain directly to the EDPS if they consider their data protection rights are not respected.[91] The role of the EDPS is important. For example, it was heard during the EU Data Protection Reform. This will be dealt more accurately in the section 3.

1.2.3 EU´s legislation on data protection in police matters

This chapter will introduce how the protection of personal data is currently regulated at the EU level in police matters. The DPD does not apply to the area of police and judicial co-

[84] EU Directive 2002/58/EC, E-privacy Directive, as amended by EU Directive 2009/136/EC amending Directive 2002/22/EC, Directive 2002/58/EC and Regulation (EC) No. 2006/2004, 25.11.2009. OJ 2009 L 337, 18.12.2009.
[85] Ibid, Article 15(1).
[86] EU Directive 2006/24/EC, Data Retention Directive.
[87] Ibid, Articles 1 & 6 and Recitals 4, 5, 7 to 11, 21 and 22.
[88] European Union Agency for Fundamental Rights and Council of Europe, 2014, p. 19.
[89] EU Regulation 45/2001, on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data.
[90] Ibid, Chapter V.
[91] Ibid, Article 41 & 46.

operation in criminal matters.[92] In 2008 the EU adopted the Council Framework Decision 2008/977/JHA[93] to protect personal data processed in the framework of police and judicial cooperation in criminal matters. It repeats the principles specified by the Convention 108 and the DPD[94] and it ensures data protection in the cross-border cooperation between these authorities and its applicability does not extend to national security. The aim is to protect natural persons´ personal data when it is processed to prevent, investigate, detect, or prosecute a criminal offence or to execute criminal penalty.[95] It incorporates a joint reference to the Charter Articles 7 and 8.[96]

The competent authorities act on behalf of the member states or the EU when working in police matters. These authorities are the EU agencies or bodies, as well as member states police, customs and other competent national authorities.[97] Only a competent authority may use the collected data and only for the purpose for which it was collected. When personal data is transferred to another member state, the recipient state must respect the restrictions on the exchange which are provided for in the transmitting state´s law.[98] The recipient may use the data for different purposes than the ones for which the data was transmitted.[99] The competent authorities must document data transmissions to enable the verification of the processing´s lawfulness and to ensure the data security. Data which is received from a member state may be transferred to third parties, but only if the first state has consented to the transfer. The data may be transferred without having this prior consent, if it is necessary to prevent an immediate threat to public security of a state.[100]

[92] EU Data Protection Directive 95/46/EC, Article 3(2).
[93] EU Council Framework Decision 2008/977/JHA, 27.11.2008.
[94] Convention 108, 1981, Article 2, Definitions and EU Data Protection Directive 95/46/EC, Article 2 Definitions.
[95] EU Council Framework Decision 2008/977/JHA, 27.11.2008, Recital 6 and Article 1(2).
[96] Ibid, Recital 48.
[97] Ibid, Article 2(h).
[98] Ibid, Article 3(1) & 12.
[99] Ibid, Article 11: Personal data received from or made available by the competent authority of another member state may, in accordance with the requirements of Article 3(2), be further processed only for the following purposes other than those for which they were transmitted or made available: (a) the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties other than those for which they were transmitted or made available; (b) other judicial and administrative proceedings directly related to the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties; (c) the prevention of an immediate and serious threat to public security; or (d) any other purpose only with the prior consent of the transmitting member state or with the consent of the data subject, given in accordance with national law. The competent authorities may also further process the transmitted personal data for historical, statistical or scientific purposes, provided that member states provide appropriate safeguards, such as making the data anonymous.
[100] Ibid, Article 10 & 13.

The data subject has the right to be informed of the collection and processing of her personal data by the competent authorities. She has the right to access to information about her data´s processing, although the access may be restricted on certain grounds such as if it is a necessary and proportional measure to avoid preventing investigations. The data subject has the right to rectification, erasure or blocking of her personal data. If the data subject is prevented from exercising her rights, she must be able to complain to the national supervisory authority or to a court. If the data subject is damaged because of violations of the national law, she must have access to a judicial remedy.[101]

The competent authorities' take different measures to protect personal data against unlawful processing. Naturally, these measures should be regulated in the national legislation and such measures are called: the equipment access control, data media control, storage control, user control, data access control, communication control, input control, recovery, reliability, and integrity.[102] Member states must make sure that independent national supervisory authorities monitor the application of the rules adopted in accordance to this Framework Decision. These supervisors hear the complaints concerning the protection of individual's rights considering the processing of their personal data.[103]

In addition to the Council Framework Decision 2008/977/JHA, the information exchange between the member states public officials is regulated by several instruments.[104] The

[101] Ibid, Articles 16 - 20.
[102] Ibid, Article 22(2): In respect of automated data processing each Member State shall implement measures designed to: (a) deny unauthorized persons access to data-processing equipment used for processing personal data (equipment access control); (b) prevent the unauthorized reading, copying, modification or removal of data media (data media control); (c) prevent the unauthorized input of data and the unauthorized inspection, modification or deletion of stored personal data (storage control); (d) prevent the use of automated data-processing systems by unauthorized persons using data communication equipment (user control); (e) ensure that persons authorized to use an automated data processing system only have access to the data covered by their access authorization (data access control); (f) ensure that it is possible to verify and establish to which bodies personal data have been or may be transmitted or made available using data communication equipment (communication control); (g) ensure that it is subsequently possible to verify and establish which personal data have been input into automated data processing systems and when and by whom the data were input (input control); (h) prevent the unauthorized reading, copying, modification or deletion of personal data during transfers of personal data or during transportation of data media (transport control); (i) ensure that installed systems may, in case of interruption, be restored (recovery); (j) ensure that the functions of the system perform, that the appearance of faults in the functions is reported (reliability) and that stored data cannot be corrupted by means of a malfunctioning of the system (integrity).
[103] Ibid, Article 25.
[104] See for example: the EU Council Framework Decision 2009/315/JHA on the organisation and content of the exchange of information extracted from the criminal record between Member States, OJ 2009 L 93, 26.2.2009.; and the EU Council Decision 2000/642/JHA, concerning arrangements for cooperation between financial intelligence units of the Member States in respect of exchanging information, OJ 2000 L 271, 17.10.2000.

member states may utilize the possibilities provided by legal tools that are established between the member states. There are several instruments providing databases to improve cooperation and information sharing between the member states national authorities (the Prüm Decision[105], the Schengen Information System[106] and the Visa Information System[107]); as well as institutions assisting in the fight against international crime and terrorism (Europol[108] and Eurosur[109]) and to promote judicial cooperation in investigations and prosecutions (Eurojust[110], the Customs Information System[111] and the Eurodac[112]).

1.3 Processing personal data and the data protection law principles

This chapter explains what it means to process personal data, what is the data subject´s consent and what are the principles guiding the data processing. The processing of personal data is imbalanced and asymmetric between the two actors of information processing: the data subject and the data controller. From the data subject´s perspective the amount of information that can be gathered is unlimited, just as is the scope of analysis that can be done from the data. The collected data can be retained forever.[113]

1.3.1 Categories of personal data and the definition of its processing

To protect a person´s personal data, first this person must be identifiable. If a piece of information contains some elements of identification by which a person can be identified directly or indirectly, the person can be considered as identifiable.[114] Information contains

[105] EU Council Decision 2008/615/JHA; Prüm Decision, 23.6.2008.
[106] EU Council Decision 2007/533/JHA, SIS-II, 12.6.2007.
[107] EU Regulation 767/2008, VIS Regulation, 9.7.2008.
[108] EU Council Decision 2009/371/JHA establishing the European Police Office, 6.4.2009.
[109] EU Regulation 1052/2013, Eurosur Regulation, 22.10.2013.
[110] The Eurojust Decisions: EU Council Decision 2002/187/JHA setting up Eurojust with a view to reinforcing the fight against serious crime, OJ 2002 L 63, 28.2.2002; EU Council Decision 2003/659/JHA amending Decision 2002/187/JHA setting up Eurojust with a view to reinforcing the fight against serious crime, OJ 2003 L 44, 18.6.2003 ; EU Council Decision 2009/426/JHA on the strengthening of Eurojust and amending Decision 2002/187/JHA setting up Eurojust with a view to reinforcing the fight against serious crime, OJ 2009 L 138, 16.12.2008.
[111] EU Council Decision 2009/917/JHA, CIS Decision on the use of information technology for customs purposes, OJ 2009 L 323, 30.11.2009.
[112] Eurodac Regulations: EU Regulation 2725/2000 concerning the establishment of Eurodac for the comparison of fingerprints for the effective application of the Dublin Convention, OJ 2000 L 316, 11.12.2000 and EU Regulation 407/2002, laying down certain rules to implement Regulation 2725/2000 concerning the establishment of Eurodac for the comparison of fingerprints for the effective application of the Dublin Convention, OJ 2002 L 62, 28.2.2002.
[113] Nissenbaum, 1998, p. 559, 576.
[114] EU Data Protection Directive 95/46/EC, Article 2 (a) "*'personal data' shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be*

personal data about a person if this person is identified in it or if she is described in a way which makes it possible to find out who she is by conducting further research.[115]

"Personal data" connects to the person's private and professional life. The European data protection law protects these both types of information in the same manner.[116] The data protection law applies irrespective of the form in which the personal data is stored or used. Cell samples of human tissue are personal data as they record a person´s DNA.[117] Written or spoken communications may contain personal data as well as images,[118] including closed-circuit television footage[119] or sound[120]. Personal data is sensitive if it may pose a risk to the data subject. Sensitive data means data revealing racial or ethnic origin, political opinions, religious or other beliefs, or criminal conviction, and data concerning health or sexual life. It may be processed only with special safeguards.[121]

The 'processing of personal data' means any operation taken upon personal data, such as "*collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction*"[122]. Data processing refers mainly to automated processing, but manual processing may be required between automated operations.[123] Heikki Partanen divides the automated data processing into two main categories: 'direct' processing where the processing begins with identification of the data subject, and 'reverse' processing where the idea of the processing is to identify the subject. The reverse processing relates to criminal procedures where individual´s actions are investigated and the outcomes end up as personal data in the information system.[124]

---

identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity."

[115] European Union Agency for Fundamental Rights and Council of Europe, 2014, p. 39.

[116] ECtHR, No. 27798/95, Amann v. Switzerland, 16.2.2000, para 65; CJEU, Joined cases C-92/09 and C-93/09, Schecke and Eifert, 9.11.2010, para 59.

[117] European Union Agency for Fundamental Rights and Council of Europe, 2014, p. 43.

[118] ECtHR, No. 59320/00, Von Hannover v. Germany, 24.6.2004; ECtHR, No. 50774/99, Sciacca v. Italy, 11.1.2005.

[119] ECtHR, No. 44647/98, Peck v. UK, 28.1.2003; ECtHR, No. 420/07, Köpke v. Germany, 5.10.2010.

[120] EU Data Protection Directive 95/46/EC, Recitals 16 and 17; ECtHR, No. 44787/98, P.G. and J.H. v. UK, 25.9.2001, paras. 59 and 60; ECtHR, No. 71611/01, Wisse v. France, 20.12.2005.

[121] Convention 108, 1981, Article 6; EU Data Protection Directive 95/46/EC, Article 8.

[122] Convention 108, 1981, Article 2(B); EU Data Protection Directive 95/46/EC, Article 2(C).

[123] Convention 108, 1981, Article 2(C) and EU Data Protection Directive 95/46/EC, Article 2(b) and 3(1).

[124] Partanen, 2016, p. 101.

The DPD defines the data controller as a person or body who determines the purposes and means of the processing of personal data. The processor then processes that data on behalf of the controller.[125] There may be several separate entities who together act as a data controller and process data for a shared purpose.[126] This is called joint controllership. The controller must specify and clarify the purpose of the processing before it begins.[127] She must either notify the supervisory authority or document it internally. Every new processing purpose must have its own legal basis. The joint controllership provides better protection to the data subject´s interests. This results in joint liabilities for damages and gives the data subject a wider range of remedies.[128]

A data subject´s consent is often the legal basis for data processing. Convention 108 does not define the consent, but rather leaves it to domestic law. EU law sets out three elements for establishing the validity of a subject´s consent. The data subject must have been under no pressure when consenting, she must have been informed of the object and consequences of consenting, and the scope of consent must be concrete.[129] She must be provided with an understandable description of the subject matter,[130] and she must re-consent if processing operations change in a way which was not foreseeable.[131] As an example of data subject´s free consent, in many airports the passengers need to go through body scanners to enter the boarding area. The scanning might be presented as an option. The passengers agree because they try to avoid problems, but the consent is not sufficiently free.[132] The DPD Article 7(E) provides basis for this: the passengers must cooperate because of an overriding public interest. They could choose between scanning and pat-down, but only as an additional measure.[133]

[125] EU Data Protection Directive 95/46/EC, Article 2(D) & (E). See also Section Definitions.
[126] Ibid, Article 17(3) and (4).
[127] Article 29 Working Party Opinion 03/2013, 2.4.2013.
[128] Article 29 Working Party Opinion 10/2006, 22.11.2006 and Article 29 Working Party Opinion 1/2010, 16.2.2010, p. 25.
[129] EU Data Protection Directive 95/46/EC, Article 2(H); and European Union Agency for Fundamental Rights and Council of Europe, 2014, p. 56.
[130] European Union Agency for Fundamental Rights and Council of Europe, 2014, p. 59.
[131] CJEU, C-543/09, Deutsche Telekom, 5.5.2011, paras 53–54.
[132] Article 29 Working Party Opinion 15/2011 , 13.7.2011, p. 15.
[133] European Union Agency for Fundamental Rights and Council of Europe, 2014, p. 58.

The E-privacy Directive separates three categories of data created during an electronic communication[134]:

- The confidential data: constituting the content of the sent messages;
- The traffic data: necessary for establishing and maintaining the communication, information of the communication partners, time and duration of the communication;
- The location data: within the traffic data, the location of the communication device.

1.3.2 Data procession must be justified, purposeful and fair

The justification of processing personal data depends on the purpose of the processing. The processing must be explained to the data subject to make sure she understands what happens to her data.[135] The DPD sets principles for the member states to further ensure that personal data is: processed fairly and lawfully; collected for specified, explicit and legitimate purposes; adequate, relevant and not excessive in relation to the purposes for which it is collected and processed; accurate and kept up to date; inaccurate or incomplete data will be erased or corrected, and; kept in a form which permits identification of data subjects as long as necessary for the purposes for which the data was collected. The data stored for historical, statistical or scientific use, must have safeguards.[136]

The OECD privacy guidelines recommend that the data controllers should be responsible for complying with data protection rules.[137] Convention 108 leaves the issue to national law and does not refer to the controllers' accountability, while the DPD states that the controllers ensure that the data protection principles are complied with.[138] The Article 29 Working Party states that controllers have an obligation to place measures to guarantee that data protection rules are followed in the processing operations and to document those measures.[139] The data processing must be fair, meaning that it is lawful, transparent and the data subjects are informed of the processing. The controllers have an obligation to make available to the data subject the copies of her data or to justify by compelling reasons for refusing to do so.[140] As an example, this violates the ECHR Article 8 if national

[134] EU Directive 2002/58/EC, E-privacy Directive, 12.7.2002, Articles 5, 6 and 9.
[135] European Union Agency for Fundamental Rights and Council of Europe, 2014, p. 74.
[136] EU Data Protection Directive 95/46/EC, Article 6(1).
[137] OECD Guidelines on governing the Protection of Privacy and transborder flows of personal data, 2013, Article 14.
[138] EU Data Protection Directive 95/46/EC, Article 6(2).
[139] Article 29 Working Party Opinion 3/2010, 13.7.2010, Para 28.
[140] ECtHR, No. 32881/04, K.H. and Others v. Slovakia, 28.4.2009, para 48.

authorities granted the access to the applicant after five years of delay, when he had requested access to a file which the secret service organization had stored on him.[141]

Interference with personal data is justified if it is based on a national law provision which is accessible to the data subjects and its effects are foreseeable.[142] The Charter Article 52 allows limitations on the processing of personal data. The Union law may provide more extensive protection and the ECHR Article 8(2) sets the minimum requirements for the lawful limitations of the right to data protection.[143] The requirements for justifiable interference are explained in the chapter 2.1, in relation to the case law of the ECtHR.

The retention of personal data must be proportionate compared to the purpose of collection and should be limited in time, especially in the police matters.[144] This means that the data collected of a suspected criminal can be stored as long as the controller has legal basis for collecting it and justification for the suspicion. Data, which is no longer needed, could be stored by anonymizing or pseudonymizing it as the time limitation applies only to personal data which is kept in a form which allows identification of data subjects.[145] Personal data can be kept in a personalized form after it no longer serves its original purpose, on grounds of using it on historical, statistical, or scientific purposes.[146] Personal data is anonymized by eliminating the identifying elements from it so the re-identification of the person is no longer possible.[147] Anonymized data is not personal data. In pseudonymization of personal data, one pseudonym replaces the identifiers, for example by encrypting the identifiers. This way personal data with encrypted identifiers can be used in many contexts, i.e. where researchers study crimes and the authorities aim to keep secret the criminals.[148] Pseudonymized data is not directly mentioned in the DPD or Convention 108.

[141] ECtHR, No. 21737/03, Haralambie v. Romania, 27.10.2009.
[142] ECtHR, No. 27798/95, Amann v. Switzerland, 16.2.2000, para 50, ECtHR, No. 23224/94, Kopp v. Switzerland, 25.3.1998, para 55, ECtHR, No. 25198/02, Iordachi and Others v. Moldova, 10.2.2009, para 50.
[143] Charter of fundamental rights of the EU, 2009, Article 52(1), see footnote 73; and ECHR, Article 8(2), see footnote 18.
[144] ECtHR, No. 30562/04 and 30566/04, S. and Marper v. UK, 4.12.2008, paras 122-124.
[145] European Union Agency for Fundamental Rights and Council of Europe, 2014, p. 73.
[146] EU Data Protection Directive 95/46/EC, Article 6(1); Convention 108, 1981, Article 5(e). See footnote 31.
[147] EU Data Protection Directive 95/46/EC, Recital 26.
[148] European Union Agency for Fundamental Rights and Council of Europe, 2014, p. 44-46.

1.4 Conclusion of the section 1

This section defined the different categories of personal data and the main principles for data processing. Basically, the processing must be justified, purposeful and fair. Often the data subject´s consent is the legal basis for legitimate processing. In relation to data processing conducted by competent authorities, the consent does not provide legal basis for the processing as the data subject is required to comply with a legal obligation.

To conclude the first section, it can already now be mentioned that the European legislation regarding the rights to the protection of personal data and privacy is well spread. These fundamental rights are primarily written in the main treaties of the EU as well as in the Charter. The EU tries to cover the field in practice by the DPD and several other instruments complementing it, although the DPD does not apply to the area of national police matters, which is the main focusing point of this paper. The EU does have the Council Framework Decision 2008/977/JHA covering this field when personal data is transferred from one member state to another. Currently Convention 108 and the CoE Data Police Recommendation guiding the Convention´s application are the only European instruments able to be applied to the work of national authorities. This will be changed in the future via the EU data protection reform. Because the technology has developed since the adoption of the DPD, the EU Commission proposed a data protection reform package in 2012. It consisted of a proposal for a GDPR[149] to replace the DPD, and of a new Data Protection Directive on Police Matters[150]. The idea of the new Directive is to replace the Council Framework Decision 2008/977/JHA and to extend the data protection principles to domestic police matters. The reform will be introduced in section 3. Before that we must go through section 2.

[149] EU Commission Proposal for a General Data Protection Regulation, COM(2012) 11 final, 25.1.2012.
[150] EU Commission Proposal for a Data Protection Directive on Police matters, COM 10 final, 25.1.2012.

2 THE EUROPEAN COURTS´ TRENDS ON DATA PROTECTION AND PRIVACY

This section introduces recent decisions of the European Courts which concern the right to the protection of personal data and the right to privacy. The first chapter lists the ECtHR rulings which have guided the understanding of personal data protection in relation to the right to respect for private life. These ECtHR cases will clarify some of the key principles of data protection. They will go through the requirements of necessary safeguards, clarify the rule of law and brighten the balances between the private and public interests and in the end, take a stand on how much a state may interfere with individual´s fundamental rights. The second chapter then turns to the CJEU rulings on the same issues. The CJEU cases are relatively recent as those derive their reasoning from the ECtHR and operate as a continuum to it. The CJEU cases focus on the Court´s approach to the Charter, as for long it was referring only to the ECHR but then transformed itself relying on to the Charter. The third chapter introduces the doctrine of margin of appreciation in Europe.

When evaluating the CJEU´s rulings on human rights issues, it is necessary to look at the ECtHR decisions. Firstly, because the Charter states that it reaffirms the fundamental rights as they result from the constitutional traditions and international obligations common to the member states, as well as from the EU´s primary law, the ECHR, the Social Charters adopted by the Community and the CoE, and the case law of both Courts (the CJEU and the ECtHR).[151] Secondly, because the CJEU leans on the ECtHR´s interpretations as can be seen in this section. These Courts approach the same themes from different angles. The ECtHR evaluates actions conducted towards an individual while the CJEU evaluates the law itself. The CJEU has not dealt a case where it would have discussed questions of data protection and the right to privacy and then balanced these with the actions of national authorities´ rights regulated by the Council Framework Decision 2008/977/JHA.[152]

2.1 The ECtHR´s recent rulings on right to privacy and data protection

This chapter will focus on the ECtHR´s judgements concerning the right to the protection of personal data and the respect of private life. The ECHR Article 8[153] grants everyone the right to respect for private life. As mentioned in the chapter 1.2 the ECHR does not

[151] Charter of fundamental rights of the EU, 2009, Preamble.
[152] Laraine, 2016.
[153] ECHR, Article 8: see footnote 18.

regulate the right to data protection, but instead Convention 108 does on a general level and the CoE Police Data Recommendation[154] guides.

2.1.1 National legislation must provide safeguards against abuse

The first so called landmark decision on this field by the ECtHR is the case *Klass and Others v. Germany*[155]. The applicants complained that German law violated their right to respect for private and family life (ECHR Article 8), as it allowed the national authorities to secretly survey individuals' mail, post and telecommunication, the data subject was not notified of the surveillance and she was not able to question the measures in the national Courts. The rule of law demands that interference by the public authorities with an individual's rights is subject to effective supervision. It must be carried out by the judiciary.[156]

The ECtHR agreed that the surveillance interfered with the applicant´s rights. The main question was whether that interference was justified under ECHR Article 8(2), which provides an exception to the right but it should be interpreted narrowly. The Court stated that terrorism threatens states, so they must be able to undertake the secret surveillance of revolutionary elements to counter such threats. The powers of secret surveillance of citizens can be tolerated only as far as is strictly necessary for safeguarding the democratic institutions. The states cannot adopt whatever measures they find appropriate, even to fight against terrorism. There must exist adequate and effective guarantees against abuses.[157] The Court found that the system was justified in the interests of national security and to prevent disorder and crime. The legislation provided adequate safeguards and conditions before a surveillance measure could be ordered.[158]

The national security interests may prevail over the individual´s interests as can be seen in the case *Leander v. Sweden*[159]. In 1979, Mr. Leander applied to work at the Naval Museum in Sweden, which was partly located in a naval base. The person to be hired had to go through a security check by the security police. Mr. Leander was rejected because of the

[154] CoE Police Data Recommendation Rec(87)15, 17.9.1987.
[155] ECtHR, No. 5029/71, Klass and Others v. Germany, 6.9.1978.
[156] Ibid, paras 25 - 26.
[157] Ibid, para 42.
[158] Ibid, paras 48 - 50,
[159] ECtHR, No. 9248/81, Leander v. Sweden, 26.3.1987.

outcome of the background check. He then complained as he did not know what information was released from the secret police-register and he did not have any access to the stored data.[160] The ECtHR found that the aim of the background check was legitimate for the protection of national security. The interference was based on a national law, it was necessary in a democratic society and foreseeable. The Court explained that the interference must correspond to a pressing social need and that it is proportionate to the aimed legitimate goal. The national authorities enjoy a wide margin of appreciation in this matter. In view of the risk that a system of secret surveillance for the protection of national security poses of undermining democracy on the ground of defending it, there must exist effective guarantees against abuse. In such case, national security may prevail over the individual interests.[161]

The evaluation of the adequacy of the safeguards is done on a case by case basis. The ECtHR stated this in the case called *Uzun v. Germany*.[162] The German authorities had suspected two individuals for their involvement in bomb attacks and surveyed them by placing a GPS device into the other man´s car. Mr. Uzun was found guilty of bomb attacks based on the evidence collected through that surveillance. He complained to the Federal Constitutional Court that his privacy was infringed, that there was no effective judicial control of this measure and the use of several means of surveillance at the same time need a separate basis in law.[163]

Because of the risk of abuse that is natural to any secret surveillance system, such measures must be based on a law that is particularly precise, especially as the available technology is becoming more sophisticated. The rule of law requires that there exist effective guarantees against abuse and the national law gives adequate protection against arbitrary interference with ECHR Article 8 rights. This assessment depends on all the circumstances of the case. These include: the measure´s nature, scope and duration; the grounds required for ordering them; the authority who is competent to allow, perform and supervise the measure; and the kind of remedy the national law provides. Investigation measures taken by different authorities must be coordinated. The Court found that the safeguards were adequate and effective: the surveillance measure was time-limited, it was

[160] Ibid, paras 1 - 15.
[161] Ibid, paras 48 - 67.
[162] ECtHR, No. 35623/05, Uzun v. Germany, 2.9.2010.
[163] Ibid, paras 6-23.

ordered by a Public Prosecutor and its extensions would have been subject to a domestic court´s review with respect to the proportionality principle. The measures were to protect national security, public safety and the rights of the victims, and to prevent crime. They were proportionate: the GPS surveillance was ordered after less intrusive methods proved insufficient, it lasted for a short period and affected the applicant only when he was in his accomplice's car (It was not total and comprehensive).[164]

2.1.2 Clarity of the rule of law includes accessibility, foreseeability and precision

When a national authority holds inaccurate personal data, the data subject should be able to correct it. In the case called *Rotaru v. Romania* the applicant complained of an infringement of his right to privacy as the Romanian Intelligence Service held personal data of him which contained wrong information, which the authorities had used, and it was impossible to correct the data.[165] The ECtHR stated that the storing of applicant´s information, it´s usage, and a refusal to allow him to correct it, interfered with his right to privacy. Such interference must be in accordance with the law, pursue a legitimate aim under the ECHR Article 8(2) and be necessary to reach that aim. The measure should have basis in national law and the law should be accessible to the person concerned, and its effects should be foreseeable. A rule must be precise to enable any individual to regulate her actions.[166] The secret surveillance systems must provide safeguards established by law which apply to the supervision of the relevant services' activities.[167]

The ECtHR discussed the foreseeability of the domestic law in the case *Malone v. UK*.[168] Mr. Malone was charged with offences relating to dishonest handling of stolen goods. During the trial, it turned out that a telephone conversation, to which he had been a party, was intercepted by the police on the authority of a warrant. He complained that the tapping of his conversations without his consent was unlawful even if done with a warrant.[169] The ECtHR repeated the definition of "law" from the case *Silver and Others v. UK*: Firstly, the law must be accessible - the citizen must be able to have an indication that is adequate in the circumstances of the legal rules applicable to a certain case; Secondly, a norm is not

[164] Ibid, paras 60-81.
[165] ECtHR, No. 28341/95, Rotaru v. Romania, 4.5.2000, paras 1 - 25.
[166] Ibid, paras 46, 48, 52 & 55.
[167] Ibid, paras 59 - 63.
[168] ECtHR, No. 8691/79, Malone v. UK, 2.8.1984.
[169] Ibid, paras 12 - 18.

law unless it enables the citizen to regulate her conduct - she must be able to foresee the consequences of an action.[170] The Court recognized the special nature of police investigations and the risk of arbitrariness when the police´s power is exercised in secret. The ECHR requirements cannot be the same when intercepting communications for police investigations as they are in other contexts. The law does not have to be such that an individual can foresee when his communications are going to be intercepted. But it must give an indication of the conditions when authorities may secretly interfere with their rights. The law must clarify the scope and manner of exercise of the executive´s legal discretion to give the individual adequate protection against arbitrary interference.[171]

National measures which interfere with individual´s fundamental rights must be based on a law that is precise. The ECtHR dealt with this issue in the case *Kruslin v. France*[172]. In 1985 Mr. Kruslin was brought before French Court. One of the evidences was a secretly recorded telephone conversation in which he had participated. Mr. Kruslin complained of violation invoking ECHR Article 8. One feature the ECtHR noticed was that the authorities had increased secret measures, like telephone tapping, because of development of serious crime.[173] Secret measures must be based on detailed provisions as the technology is becoming more sophisticated. The French Government stated that the law had seventeen safeguards which related either to the carrying out the measure or to the usage of the results. The ECtHR found them as only partly written to the legislation and the rest was out of individual´s access. Also, there was no rule which would oblige a judge to set a limit on the duration of tapping and there was no definition of the nature of crimes which may give rise to such an order, or when the recordings must be erased. The Court found that the national practice lacked clarity and necessary regulatory control.[174]

2.1.3 Interference with private life should be restricted to only what is necessary

A measure which interferes with an individual´s fundamental right may be necessary to enable the protection of others´ rights and the public interest. In the *Köpke*[175] case the

[170] ECtHR, No. 5947/72; 6205/73; 7052/75; 7061/75; 7107/75; 7113/75, Silver and Others v. UK, 25.3.1983, para 87-88.
[171] ECtHR, No. 8691/79, Malone v. UK, 2.8.1984, paras 66-68.
[172] ECtHR, No. 11801/85, Kruslin v. France, 24.4.1990.
[173] Ibid, paras 8-20.
[174] Ibid, paras 30-36.
[175] ECtHR, No. 420/07, Köpke v. Germany, 5.10.2010.

applicant, a supermarket cashier, was fired from her job for theft. Her employer had run a secret video surveillance operation. The conducts of the applicant and her colleague were secretly recorded at their workplace. The collected images were examined by fellow employees and used in the proceedings at the German Courts.[176] The ECtHR stated that the interference with privacy was restricted to what was necessary. The surveillance had been carried out after losses had been detected. The measure was targeted to only two suspected workers. It was limited in time and covered only public places. The data was not disclosed to outsiders and it was used only for the termination of her employment and in the Courts. The ECtHR mentioned that the balance which the authorities had struck between the interests at issue is not the only way for them to comply with their obligations under the ECHR. In the future, these competing interests may get different weights as new technologies enable more extensive intrusions into private lives.[177]

Storage of personal data in a blanket and indiscriminate nature is unnecessary, especially if there is no difference between the treatments of innocent persons to the convicted ones. The ECtHR dealt a case called *S. and Marper v. UK*[178], where the issue was whether the retention of the personal data of the applicants was necessary, as those persons had been suspected of criminal offences, but not convicted. The applicants´ personal biometric data (meaning fingerprints, cellular samples and DNA profiles) was stored by the UK police, the domestic law allowed an unlimited retention, and the acquitted persons were not able to request deletion of their data.[179]

The ECtHR noted that the domestic legislation cannot provide for every eventuality. The required level of precision depends on the content of the instrument in question, the field it covers and the number and status of those to whom it is addressed. Detailed rules are necessary to govern the scope and application of measures, as well as minimum safeguards concerning duration, storage, usage, third parties´ access, procedures for guarding the integrity and confidentiality of data and procedures for its destruction. These provide sufficient guarantees against the risk of abuse and arbitrariness.[180]

[176] Ibid, Chapter 2.
[177] Ibid, p. 11-13.
[178] ECtHR, No. 30562/04 and 30566/04, S. and Marper v. UK, 4.12.2008.
[179] Ibid, paras 51 - 52 & 60.
[180] Ibid, paras 96 & 99.

The Court reasoned that the UK is in the vanguard of the development of the use of DNA samples in the detection of crime. The other CoE member states have set limits on the retention and use of such data to achieve a proper balance with the competing interests. The protection provided by the ECHR Article 8 would be unacceptably weakened if the use of modern scientific techniques in the criminal-justice system were allowed at any cost. The possible benefits of the use of these techniques must be balanced against privacy interests. The consensus among the CoE states in this respect narrows the margin of appreciation left to the UK to set the permissible limits of the interference with privacy. A state which is acting as a pioneer in the development of new technologies bears special responsibility for striking the right balance in this regard.[181]

The Court stated that the legitimate interest in the prevention of serious crime might outweigh the interests of the individuals and the community in protecting personal data. But the Court was "*struck by the blanket and indiscriminate nature of the power of retention*" in the UK. The data could be stored irrespective of the nature of the suspected offence or of the age of the suspected person; the retention was not time-limited; there was only limited possibilities for an acquitted individual to have the data removed from the database; and there is no provision for independent review of the justification for the retention. The Court ruled that such practice interfered disproportionately with the applicant´s privacy and was not necessary in a democratic society.[182] It creates a vicious circle when the authorities use secret surveillance techniques to combat serious crime. At the same time individuals develop data-protection means to prevent unauthorized parties, including authorities, to access their data.[183]

2.2 The CJEU´s recent rulings on right to privacy and data protection

This chapter introduces recent judgements by the CJEU concerning the protection of the privacy and personal data. Before 2000, the CJEU had recognized rights which corresponded to those of the ECHR, while considering the member states´ constitutional traditions. By adopting the Charter the EU shifted from a unitary system of recognition of applicable fundamental rights to a structurally binary one. This created legal uncertainty. First, the Charter and the ECHR do not have identical provisions on rights or on their

[181] Ibid, paras 111–112.
[182] Ibid, paras 118 - 126.
[183] Cocq, 2016, p. 184.

limitations. Secondly, the Charter was not binding in the beginning. Thirdly, the Charter did promote new rights.[184] The protection of personal data in national investigative authorities' work is not currently regulated at the EU level, except what falls under the scope of the Council Framework Decision 2008/977/JHA. The CJEU has not yet referred to this instrument. That is why the following cases circulate around the topic of the thesis as they are trying to find trends from the Court´s rulings to predict how the Court will respond when the data protection reform instruments begin to apply in 2018. The cases are in a chronological order due to the change of CJEU´s approach towards the Charter.

2.2.1 CJEU on protection of personal data before 2009

In 2008 the CJEU referred for the first time to the Charter and recognized the existence of a right to personal data protection in the *Promusicae* case.[185] The Court used the Charter to identify a fundamental right which had never been recognized as integral to the general principles of EU law, even though the Charter was not yet legally binding.[186] In 2008 the Charter already existed but the Union courts still had to consider the ECtHR case law when dealing with fundamental rights issues. The CJEU found it possible to refer to the Charter Article 8 as there was a mention of the Article in the preamble of the E-Privacy Directive[187]. The *Promusicae* case was about various EU provisions whether they required member states to lay down an obligation to communicate personal data to ensure effective protection of copyright in the context of civil proceedings. The Court stated that the Charter's Article 7 "*substantially reproduces*" the ECHR Article 8, and the Charter Article 8 "*expressly proclaims the right to protection of personal data*".[188] The recognition of the right to personal data protection in the Charter's Article 8 did not influence the reasoning of the Court´s judgment. Instead the Court considered the right to data protection as classified under the right to respect for private life.[189]

In 2008 the CJEU dealt with a case called *Satamedia*[190] which concerned a reference to the DPD. The Court stated that the DPD´s objective, to protect individuals´ fundamental rights

[184] Fuster, 2014, p. 213.
[185] CJEU, C-275/06, Promusicae, 29.1.2008, Para 64.
[186] Fuster, 2014, p. 226.
[187] EU Directive 2002/58/EC, E-privacy Directive, 12.7.2002.
[188] CJEU, C-275/06, Promusicae, 29.1.2008, para 64. About the Charter, see Chapter 1.2.1.2.
[189] Fuster, 2014, p. 227.
[190] CJEU, C-73/07, Satamedia, 16.12.2008.

and their right to privacy, must be matched with the right to freedom of expression.[191] The Advocate General´s opinion in the case shows the connection between the CJEU and the ECtHR judgements on human rights questions. The Advocate General noticed the existence of the Charter´s protection of personal data but stated that the Union courts must consider the ECtHR case law when dealing with fundamental rights issues.[192]

In 2009 the CJEU discussed the individual´s right to have access to her personal data in the case called *Rijkeboer*.[193] Mr. Rijkeboer had asked a College in Rotterdam to give information about the disclosure of his personal data to third parties from the last two years. The College gave him information only for one of the years.[194] In its judgement, the CJEU did not refer to the Charter or to the right to the protection of personal data. The Court pointed out that the right to privacy was written in DPD Article 1 and its importance was mentioned in the preamble. The right to privacy suggested that the data subject may be sure that his personal data is processed in a correct and lawful manner, which requires that his data is accurate and disclosed only to authorized recipients.[195] This reasoning refers to the ECHR Article 8 but the CJEU linked it to the right of access established by the DPD.[196] The Advocate General stated in his opinion that the right to privacy had found its legislative expression in the DPD, the provisions of which were codified in the Charter Article 8.[197]

2.2.2 CJEU on data protection after 2009

Since 2009, after the Charter received its legally binding status, the CJEU attempted to place the new Charter Article 8 right into the previous case law, which had been marked by a connection between the EU´s personal data protection and the ECHR Article 8. The case *Schecke and Eifert*[198] shows the Court´s willingness to begin ruling based on the Charter while at the same time using the ECHR and the ECtHR´s case law. The CJEU stated that

[191] CJEU, C-73/07, Satamedia, 16.12.2008, para. 52-56.
[192] CJEU, C-73/07, Opinion of advocate General Kokott, on case Satamedia, 8.5.2008, paras 37 & 40.
[193] CJEU, C-553/07, Rijkeboer, 7.5.2009.
[194] Ibid, para 4.
[195] Ibid, paras 46-49.
[196] Fuster, 2014, p. 229. And CJEU, C-553/07, Rijkeboer, 7.5.2009, para 50.
[197] CJEU, C-553/07, Opinion of Advocate General Ruiz-Jarabo Colomer, on case Rijkeboer, 22.12.2008, paras 8 & 20. About the Charter, see Chapter 1.2.1.2.
[198] CJEU, Joined cases C-92/09 and C-93/09, Schecke and Eifert, 9.11.2010.

the TEU Article 6(1)[199] gives the Charter the same value as the Treaties. The validity of the rules in question had to be evaluated based on the Charter and Charter Article 8(1) gives everyone the right to the protection of personal data. The Court saw this right as closely connected to the Charter Article 7 right to respect for private life.[200] It combined the Charter Articles 7 and 8 to create an unprecedented right, the right to respect for private life regarding the processing of personal data. It describes the right to data protection as provided by Charter Article 8(1) allowing it to act in tandem with the rules set out in Charter Articles 8(2) and 52(1), and the ECHR Article 8(2).[201] The Advocate General considered in her opinion that the two rights referred to in the case were the right to respect for private life by the ECHR Article 8 and the right to data protection by Convention 108, and that these rights were similar to the Charter Articles 7 and 8.[202]

In the case called *Scarlet*[203] the CJEU for the first time made its main reference to Charter Article 8. An Internet Service Provider (ISP) company Scarlet Extended SA was forced to implement a system for filtering and blocking electronic communications. The Court was asked to interpret EU law referring to the ECHR Article 8 (respect of private life) and Article 10[204] (freedom of expression). The Advocate General advised the Court to interpret the Charter in the light of the ECHR. The ECHR Article 8 corresponds to the Charter Articles 7 and 8 and the ECHR Article 10 corresponds to the Charter Article 11.[205] The Charter rights need to be interpreted similarly with the ECHR.[206] The Advocate General prioritized the Charter to interpret the EU data protection laws. It linked them to both the

[199] TEU, Article 6(1): The Union recognizes the rights, freedoms and principles set out in the EU Charter, which shall have the same legal value as the Treaties. The provisions of the Charter shall not extend in any way the competences of the Union as defined in the Treaties. The rights, freedoms and principles in the Charter shall be interpreted in accordance with the general provisions in Title VII of the Charter governing its interpretation and application and with due regard to the explanations referred to in the Charter, that set out the sources of those provisions.
[200] CJEU, Joined cases C-92/09 and C-93/09, Schecke and Eifert, 9.11.2010, paras 45-47.
[201] Fuster, 2014, p. 235.
[202] CJEU, Joined Cases C-92/09 and C-93/09, Opinion of Advocate General Sharpston on case Schecke and Eifert, 17.6.2010, para 71.
[203] CJEU, C-70/10, Scarlet, 24.11.2011.
[204] ECHR, Article 10: 1. Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. This Article shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises. 2. The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary.
[205] CJEU, C-70/10, Opinion of Advocate General Cruz Villalón in case Scarlet, 14.4.2011, paras 30 - 34.
[206] Charter of fundamental rights of the EU, 2009, Article 52(3): See footnote 73.

right to protection of personal data and the right to respect for private life and not only to the right to the protection of personal data.[207] The Court focused on the fact that the question was about protection of the right to intellectual property and this right´s protection must be balanced against other fundamental rights.[208] The system for filtering and blocking electronic communications might violate the customer´s rights to protection of their personal data and freedom to receive or impart information protected by the Charter.[209]

In 2011 at the *Deutsche Telekom*[210] case the CJEU claimed for the first time that the purpose of the DPD is to ensure the right to protection of personal data.[211] The Court stated that the E-Privacy Directive clarifies and supplements the DPD. The Charter Article 8(2) allows the processing of personal data if conditions are met (fairly, for specified purposes and based on the consent of the person concerned, or another legitimate basis).[212]

Then in October 2012 the CJEU turned more towards the Union´s own legislation. In the CJEU case *Commission v Austria*[213] the question was about the independence of an Austrian data protection authority. The Court found that processing of personal data has to be subjected to control by an independent authority and this is based on the primary law of the EU, the Charter Article 8(3) and the TFEU Article 16(2).[214]

2.2.3 Data retention must be balanced to the aim pursued

The CJEU and the ECtHR have similar approaches to the requirement of safeguards on measures interfering with an individual´s fundamental rights. In the case of *Digital Rights Ireland*, which was a joined case, the CJEU had to examine the validity of the Data Retention Directive 2006/24/EC[215] in the light of the Charter Articles 7 and 8 and the question of the validity of the Directive.[216] The first case refers to a situation when Digital Rights (Irish digital rights lobbying group) asked the national court to declare the invalidity

[207] Fuster, 2014, p. 237. About the Charter, see Chapter 1.2.1.2.
[208] CJEU, C-70/10, Scarlet, 24.11.2011, paras 43–46.
[209] Ibid, paras 50–51.
[210] CJEU, C-543/09, Deutsche Telekom, 5.5.2011.
[211] The case interprets the EU Directives Universal Services Directive 2002/22/EC and the E-privacy Directive 2002/58/EC, in relation to proceedings of the obligations of companies´ assigning telephone numbers to make available to other parties' data related to subscribers.
[212] Ibid, paras 49-52. About the Charter, see Chapter 1.2.1.2.
[213] CJEU, C-614/10, Commission v Austria, 16.10.2012.
[214] Ibid, para 36. About the Charter and the TFEU, see Chapters 1.2.1.1 and 1.2.1.2.
[215] EU Directive 2006/24/EC, Data Retention Directive, 15.3.2006. OJ 2006 L105, 13.4.2006.
[216] CJEU, Joined cases C-293/12 and C-594/12, Digital Rights Ireland, 8.4.2014, para 23.

of the Data Retention Directive and part of a national law. These require the providers of telephone communications services to retain users´ traffic and location data to prevent and investigate crime and to protect state security. The second case asked whether the Data Retention Directive complies with the Charter as it allows the retention of data in relation to an unlimited number of persons for a long time. The retention mainly affects persons whose actions do not justify the retention of their data.[217]

The EU legislation which deals with interference of fundamental rights, must lay down clear and precise rules to set minimum safeguards. These must also govern the scope and application of a measure and the need for safeguards is greater when personal data is processed automatically. The protection of the right to privacy requires limitations in relation to the protection of personal data to apply only as far as strictly necessary. This is not fulfilled by legislation which authorizes to retain all personal data which has been transferred from the EU to the US. The legislation should have differentiation, limitation or exception in light of the aimed objective. The purposes must be specific, restricted and justify the interference with that data.[218] The Court did not rule that the general retention was illegal as such but it is against it and found the Data Retention Directive to be invalid. The judgement listed 13 problems in the Directive which are either reasons for annulment or requirements for the retention to be proportionate.[219] The Directive does not have clear rules governing the scope of the interference with the rights of the Charter. It does not have rules which would be adapted to the huge amount of data which it orders to be retained, nor rules to secure the data to ensure integrity and confidentiality, nor does it oblige the member states to provide these rules.[220]

The EU Commission will not propose a new Data Retention Directive but it monitors the legislative developments´ at a national level. After the *Digital Rights Ireland* decision, some states adopted new laws which are similar to the annulled Data Retention Directive and some remained with their old laws. If the Commission acts politically and refrains from acting in case of an infringement, it prevents the Charter from protecting privacy.[221]

[217] Ibid, paras 17 & 20.
[218] Ibid, paras 52 - 61.
[219] Vainio, 2016, p. 232 & 247.
[220] CJEU, Joined cases C-293/12 and C-594/12, Digital Rights Ireland, 8.4.2014, paras 65 - 71. About the Charter, see Chapter 1.2.1.2.
[221] Vainio, 2016, p. 253.

2.2.4 General access to the content of communications violates privacy

Legislation which allows the authorities to access to the content of electronic communications on a generalized basis violates the core of the right to privacy. When personal data is transferred to a third country, an adequate level of protection of privacy must be ensured. In the CJEU case *Schrems*[222], Mr. Schrems had complained to the Irish Data Protection Commissioner about the fact that Facebook Ireland Ltd transfers every Facebook user´s personal data to the mother company in the USA. The transfers were conducted under the Safe Harbour Arrangement[223]. Mr. Schrems asked the Irish Commissioner to prohibit Facebook Ireland from transferring his personal data to the US. He claimed that the law and practice in the US does not protect personal data adequately against the public authorities´ surveillance activities. The Commission refused to investigate the matter.[224]

The question in the case regarded sending personal data from an EU member state to a third country under the DPD Article 25[225]: personal data may be transmitted from a member state to a third country if the receiving state ensures adequate protection of the data. Article 25(2) states that the adequacy of the protection is assessed "*in the light of all the circumstances surrounding a data transfer*". The circumstances considered in the assessment are listed in the DPD and the Council Framework Decision 2008/977/JHA: to the nature of the certain data, the processing´s duration and purpose, the data´s state of origin and the state of destination, the complied with professional rules and security measures in the third country and the rules of law in force.[226]

[222] CJEU, C-362/14, Schrems, 6.10.2015.
[223] EU Commission Decision, 2000/520/EC, pursuant to Directive 95/46/EC on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce, OJ L 215, 25.8.2000, 26.7.2000.
[224] CJEU, C-362/14, Schrems, 6.10.2015, paras 2 & 27 - 29.
[225] EU Data Protection Directive 95/46/EC, Article 25: 1. The Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive, the third country in question ensures an adequate level of protection. 2. The adequacy of the level of protection afforded by a third country shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations; particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in that country.
[226] EU Data Protection Directive 95/46/EC, Article 25(2-3) and EU Council Framework Decision 2008/977/JHA, 27.11.2008, Article 13(4).

The CJEU spent roughly two-thirds of its decision on the question of the supervisory authority´s powers.[227] The Court noted that the national supervisory authorities monitor the compliance with the EU rules concerning the protection of individuals when their personal data is processed. The supervisory authorities have the powers to check whether a transfer of personal data from its own member state to a third country complies with the DPD´s requirements, and they are obliged to investigate the complaints.[228]

The Court stated that the adequate level of protection requires the third country to ensure, by its domestic law or its international commitments, a level of protection of rights and freedoms that is "*essentially equivalent*"[229] to that guaranteed within the EU. It does not have to be identical. The Advocate General added in her opinion that the Commission must also examine the way that the third country protects the personal data in practice.[230] The CJEU underlined that if the authorities have general access to the content of electronic communications, it compromises the essence of the right to privacy.[231] The English version of the judgement uses the term "*compromises the essence*", while the Finnish translation uses a sterner term. It states that such access "violates" (in Finnish "loukkaa").

The Court refrained from being political however, as it did not look at the national US legislation. Instead it noted that the Safe Harbor Arrangement itself does not limit the interference with the fundamental rights of the persons whose data is transferred from the EU to the US.[232] The US authorities can process that data in a way which is against the purposes for which it was transferred, and more than is proportionate to protect national security. The Charter is the key when evaluating the compliance of the requirements laid down in the DPD, along with the interference of fundamental rights. The data transfers under the Arrangement are invalid.[233] There were three things lacking in terms of legal remedies, of regular monitoring in the U.S., and of balance between a nation's interests and fundamental rights.[234]

[227] Bräutigam, 2016, p. 155.
[228] Ibid, paras 41, 47–49 & 63.
[229] CJEU, C-362/14, Schrems, 6.10.2015, para 73.
[230] CJEU, C-362/14 Opinion of Advocate General, on case Schrems, 25.9.2015, para. 227.
[231] CJEU, C-362/14, Schrems, 6.10.2015, paras. 92 - 94.
[232] Bräutigam, 2016, p. 155.
[233] CJEU, C-362/14, Schrems, 6.10.2015, paras 88 - 98 and 106; And CJEU, Joined cases C-293/12 and C-594/12, Digital Rights Ireland, 8.4.2014, para 39.
[234] Bräutigam, 2016. p. 166.

2.2.5 Retained data needs a relationship with the threat to public security

In 2016 the CJEU stated that the retention of personal data to fight against serious crimes should happen because that data has a connection with a crime. In the Case *Tele2 Sverige AB*[235] the company Tele2 (a provider of electronic communications services) was required to retain traffic and location data of its users under the Data Retention Directive[236], but not the content of those communications. The retained data makes it possible to identify the communication equipment and to establish its location, to identify the communication´s date, time, duration and type, and to track the source of the communication and its destination.[237] Tele2 stated that it will cease to retain the data because of the CJEU decision *Digital Rights Ireland*. The Swedish police complained about Tele2´s conduct and a Swedish Court requested for a preliminary ruling from the CJEU. The CJEU dealt with the question whether a general obligation to retain everyone´s traffic data without distinctions, limitations or exceptions to fight crime, is compatible with the E-Privacy Directive Article 15(1)[238], taking into account the Charter Articles 7, 8 and 52(1).[239] The Court stated that the list in the E-Privacy Directive Article 15 is exhaustive, and that measures may derogate from the principle of confidentiality "*to safeguard national security — that is, State security — defence, public security, and the prevention, investigation, detection and prosecution of criminal offences…*"[240].

The Court stated that the protection of the right to respect for private life requires that derogations from and limitations on the protection of personal data apply only to what is strictly necessary. The retention of data should be an exception, and national legislation which makes the retention of data a rule on a general basis exceeds these limits and is not justified. There must be a relationship between the retained data and a threat to public

[235] CJEU, Joined cases C-203/15 and C-698/15, Tele2 Sverige AB, 21.12.2016.
[236] EU Directive 2006/24/EC, Data Retention Directive, 15.3.2006. OJ 2006 L105, 13.4.2006.
[237] CJEU, Joined cases C-203/15 and C-698/15, Tele2 Sverige AB, 21.12.2016, para 98.
[238] EU Directive 2002/58/EC, E-privacy Directive, 12.7.2002, Article 15(1): Member States may adopt legislative measures to restrict the scope of the rights and obligations provided for in Article 5, Article 6, Article 8(1), (2), (3) and (4), and Article 9 of this Directive when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defense, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorized use of the electronic communication system, as referred to in Article 13(1) of Directive 95/46/EC. To this end, Member States may, inter alia, adopt legislative measures providing for the retention of data for a limited period justified on the grounds laid down in this paragraph. All the measures referred to in this paragraph shall be in accordance with the general principles of Community law, including those referred to in Article 6(1) and (2) of the Treaty on European Union.
[239] CJEU, Joined cases C-203/15 and C-698/15, Tele2 Sverige AB, 21.12.2016, paras 1, 17 & 44-51.
[240] Ibid, para 90.

security. The action must be based on evidence of a certain individual whose data might expose a link with serious crimes and to help to fight these crimes or prevent a risk to public security.[241] The national retention measure must have clear rules regarding the circumstances when the electronic communications services provider must give the national authorities access to the data. With the objective of fighting serious crimes, access may be given to only the data of individuals who are suspected of being involved in a serious crime. The authorities´ request to access should be reviewed by an independent body before the access.[242]

2.3 The margin of appreciation in Europe

The term "margin of appreciation" refers to the freedom of action a government enjoys when it evaluates factual situations and applies the rules of treaties.[243] This chapter shall introduce how it was formulated in the ECtHR´s case law and how the CJEU has approached the issue in relation to data protection. The ECtHR allows states to have a degree of discretion when it acts in the area of an ECHR right, when the Court has to consider if that state has breached the ECHR. This doctrine is called the margin of appreciation and the ECtHR developed it through its case-law. The ECtHR recognizes that member states interpret the ECHR differently based on their legal and cultural traditions. The margin of appreciation enables the Court to balance the sovereignty of member states with their obligations under the Convention.[244]

The margin of appreciation given to the member states can be either narrow or wide, depending of the case at hand and the rights and freedoms involved. The margin is usually considered as narrow when the question is of a person's identity or existence[245]. If the member states are not able to form a consensus on certain issues the ECtHR may consider that the matter is best left to individual states.[246] The margin of appreciation is wide when the aim is to protect national security.[247] It is also wide if the member states have not formed a consensus on the issue at question and what would be the best way to protect it,

[241] Ibid, paras 96, 104–107, 111.
[242] Ibid, paras 117–121.
[243] Arai-Takahashi, 2001, p. 2.
[244] ECHR Reform, Margin of Appreciation, An overview of the Strasbourg Court's margin of appreciation doctrine. www.justiceinitiative.org , 2012.
[245] ECtHR, No. 6339/05, Evans v. UK, 7.3.2006, About the ECHR Article 2, the right to life.
[246] ECtHR, No. 2346/02, Pretty v. UK, 29.4.2002.
[247] ECtHR, No. 5029/71, Klass and Others v. Germany, 6.9.1978.

as well as if the member state must balance between competing interests or ECHR rights.[248] The CoE member states do not have a common agreement as to what the "state security" means as it depends on national policies.[249]

It is for the national Courts to primarily interpret and apply the domestic law and the ECtHR should not rule on whether a national measure complies with national law.[250] The national authorities are in principle in a better position than an international judge to give an opinion of the necessity to restrict (for an example) the freedom of expression to protect public morals.[251] A serious reason must exist before public authorities may interfere in an area covered by ECHR Article 8, where private life is at stake.[252]

The doctrine is recognized in CJEU practice, which has applied it in number of areas and it has developed jurisprudence involving the protection of fundamental rights. The CJEU has applied the doctrine frequently for interpreting the public security exception, for example in relation to the freedom of movement of workers[253]. The Court has recognized that these exceptions must be read similarly to the limitation clauses of ECHR Articles 8-11.[254] The EU member states may use personal data for, among other aspects, the prevention of an immediate threat to public security.[255] The national authorities may interfere with person´s fundamental rights if it is based on national security and public interest requirements. To establish the existence of an interference with privacy, it does not matter if the data is sensitive or if the data subject suffers because of that interference.[256] In the CJEU case *Tele2 Sverige AB*[257], the Court dealt with a matter in which one party of the case was a

[248] ECtHR, No. 6339/05, Evans v. UK, 7.3.2006.
[249] Prof. Cannataci & Dr. Caruana, 2013, p. 48.
[250] ECtHR, No. 11801/85, Kruslin v. France, 24.4.1990, para 29.
[251] ECtHR, No. 5493/72, Handyside v. UK, 7.12.1976, para 48.
[252] ECtHR, No. 7525/76, Dudgeon v UK, 22.10.1981.
[253] EC Treaty, Treaty establishing the European Community, OJ C 325, 24.12.2002, p. 33–184, 2002, Article 39: 1. Freedom of movement for workers shall be secured within the Community. 2. Such freedom of movement shall entail the abolition of any discrimination based on nationality between workers of the member states as regards employment, remuneration and other conditions of work and employment. 3. It shall entail the right, subject to limitations justified on grounds of public policy, public security or…
[254] Arai-Takahashi, 2001, p. 4-5.
[255] EU Council Act 2000/C 197/01, 29.5.2000, Article 23: 1. Personal data communicated under this Convention may be used by the Member State to which they have been transferred: a) for the purpose of proceedings to which this Convention applies; b) for other judicial and administrative proceedings directly related to proceedings referred to under point (a); c) for preventing an immediate and serious threat to public security; d) for any other purpose, only with the prior consent of the communicating Member State, unless the Member State concerned has obtained the consent of the data subject. This Article shall also apply to personal data not communicated but obtained otherwise under this Convention.
[256] CJEU, Joined cases C-293/12 and C-594/12, Digital Rights Ireland, 8.4.2014, para 33.
[257] CJEU, Joined cases C-203/15 and C-698/15, Tele2 Sverige AB, 21.12.2016.

national investigative authority. The Court did not evaluate the authority´s actions but rather EU law and the national law based on that EU law. This is because national law and national authorities´ actions are within the sovereignty of the state. In the future, the adoption of the Data Protection Directive on Police Matters is likely to change this situation, as it will step into the member states´ sovereignty.

2.4 Conclusion of the section 2

This section introduced influential cases of both Courts and their findings on questions relating to the protection of personal data and its connection to the right to respect for private life. Basically, the question was usually about balancing these rights when they are in conflict with some actions conducted by the public authorities. In conclusion, these cases laid out some of the key principles of data protection in practice.

The authorities may interfere with an individual´s fundamental right when fighting crimes, but states cannot adopt whatever measures they find appropriate. Already in 1990, the national authorities justified their actions by the increase of serious crimes and the ECtHR explained its reasoning with the development of surveillance technology[258]. 30 years later the problem is still the same. The authorities fight against terrorism and the name of the game is to balance between two interests: the protection of fundamental rights and national security. It is left to the discretion of EU member states to adopt legislation on this matter. Some states are more protective of the privacy, others more willing to protect national security.[259] The Courts have been prudent with new technologies which enable wider possibilities for the authorities to interfere with individuals´ privacy.

The interference is justified and in accordance with the law if it is based on a national provision which is precise, accessible to the concerned persons and its effects are foreseeable – so an individual can regulate her conduct based on it. The required level of precision depends on the subject matter. The law must have clear rules to govern the scope and application of interfering measures. It must have minimum safeguards concerning, inter alia, duration, storage, usage, third parties´ access, procedures for guarding the integrity and confidentiality of data and procedures for its destruction. The interference

[258] ECtHR, No. 11801/85, Kruslin v. France, 24.4.1990.
[259] Cocq, 2016, p. 193-194.

must refer to a pressing social need and be proportionate to the pursued legitimate aim. The data subject must be able to rely on that her data is processed in a lawful manner and disclosed only to the authorized recipients. If there are faults in her data, she must be able to fix it. Retained personal data must have at least some kind of a relationship to public security. The need for safeguards is greater when personal data is processed automatically.

The CJEU has based its reasoning of the right to data protection and the right privacy to the interpretations of the ECtHR. That is why the CJEU cases in this section focused on explaining the evolution of the Charter´s role in relation to these rights in question. The Union courts must consider the ECtHR case law when dealing with fundamental rights issues.[260] In the beginning the CJEU did not mention the Charter in its rulings but focused only on the ECHR. Then it began to find ways to refer to it and in 2009 when the Charter acquired the status of primary EU law, the CJEU began to move towards the Charter and in 2016 it became the key instrument in interpreting the rights to data protection and privacy.

In the ECHR system, Article 8 (the right to respect for private and family life) guarantees data protection and this right must be applied while recognizing the scope of other competing rights. Both Courts have ruled in several judgements that it is necessary to exercise balance with other rights when applying the ECHR Article 8 and Charter Article 8.[261] These are the right to the freedom of expression[262], to the freedom of arts and sciences[263] and to the protection of property[264], among others. As this is not in the focus of this thesis, these conflicts are not going to be dealt more.

[260] CJEU, C-73/07, Opinion of advocate General Kokott, on case Satamedia, 8.5.2008, para 40.
[261] See for an example the decisions: ECtHR, No. 40660/08 and 60641/08, Von Hannover v. Germany (No. 2) [GC], 7.2.2012; CJEU, Joined cases C-468/10 and C-469/10, Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) & Federación de Comercio Electrónico y Marketing Directo (FECEMD) v. Administración del Estado, 24.11.2011, para 48.; CJEU, C-275/06, Promusicae, 29.1.2008, para. 68.
[262] CJEU, C-73/07, Satamedia, 16.12.2008; ECtHR, No. 39954/08, Axel Springer AG v. Germany [GC], 7.2.2012, and ECtHR, No. 40660/08 and 60641/08, Von Hannover v. Germany (No. 2) [GC], 7.2.2012.
[263] European Union Agency for Fundamental Rights and Council of Europe, 2014, p. 30, and ECtHR, No. 10737/84, Müller and Others v. Switzerland, 24.5.1988.
[264] ECtHR, No. 36769/08, Ashby Donald and others v. France, 10.1.2013.

3 FUTURE CHANGES OF THE EU'S POLICE DATA PROTECTION LEGISLATION

This section introduces how the EU´s legislation on data protection is changing in police matters. The Data protection reform, as it is called, is on its way in the EU. The Union has adopted the GDPR[265] and the Data Protection Directive on Police Matters[266], and they both will come into force in May 2018. As explained in the introduction, this thesis focuses on the Data Protection Directive on Police Matters which is currently being implemented in the member states.

The main question of this thesis is if the forthcoming Data Protection Directive on Police Matters ensures protection for individual´s right to privacy when the national public officials process her personal data. It will not be answered yet. This section explains how the rights of the national authorities to process personal data are changing, how privacy is being protected in the changing data protection legislation, and finally the Data Protection Directive on Police Matters will be introduced.

The data protection legislation needed development as the EU had to react to the challenge posed by the increasing exchange of personal data and the need to protect the privacy. The CJEU has stated that the DPD´s objectives are to ensure that the individuals´ rights and freedoms are being protected when their personal data is processed, that the processing is uniform in member states and that the national laws ensure protection. The harmonization of the laws aimed to be complete.[267] This aim did not fully work in the real life and the Union needed a data protection reform.

3.1 The writing process of the Data Protection Directive on Police Matters

This chapter will explain the writing process of the new Data Protection Directive on Police Matters in detail and the main changes the Directive will bring along with it. This chapter explains also why the Directive was necessary and what characteristics it has.

[265] EU Regulation 2016/679, General Data Protection Regulation, 27.4.2016.
[266] EU Data Protection Directive on Police Matters 2016/680.
[267] CJEU, Joined cases C-468/10 and C-469/10, Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) & Federación de Comercio Electrónico y Marketing Directo (FECEMD) v. Administración del Estado, 24.11.2011, para 28-29.

3.1.1 Steps towards the Data Protection Directive on police matters

The road towards the new Data Protection Directive on Police Matters has been long and interesting after the DPD was adopted in 1995. It took 15 years for the EU Commission to announce its aim to propose a revision of the EU legal framework for data protection. After the 9/11 attack in US in 2001, the EU Parliament was requesting the adoption of a horizontal legal instrument like the DPD for the third pillar, the area of freedom security and justice, for many years without success. The Parliament had also attempted to authorize the data protection authorities in relation with the third pillar policies, but with limited success.[268] Convention 108 stayed as the main instrument for personal data protection in this field, as the member states had ratified it and it had references to third pillar measures. For instance, it was granted a key role in the context of the establishment of Eurojust[269] and the Prüm Decision[270].

The Declaration No 21 annexed to the Final Act of the Intergovernmental Conference which adopted the Treaty of Lisbon[271] recognized that the specific rules to protect personal data and it´s free movement in police cooperation may be necessary because of the specific nature of those fields.[272] The TFEU Article 16(2) enables the Parliament and the Council to legislate on data protection across the EU law applying to all EU policies.[273] This allows them to replace the DPD. The TFEU Article 16 refers to the free movement of personal data and the link to the right to the protection of personal data. The free movement of personal data effects indirectly the interpretation of Charter Article 8.[274] In accordance with TFEU Article 16, the Council shall adopt a decision setting the rules to protect the individuals when their data is processed by the member states, when the states are performing duties within the scope of common foreign and security policies, and the rules on that data´s free movement.[275] This sentence refers to the Council Framework Decision

[268] Fuster, 2014, p. 220.
[269] EU Council Decision 2002/187/JHA setting up Eurojust with a view to reinforcing the fight against serious crime, OJ 2002 L 63, 28.2.2002, Article 14(2).
[270] EU Council Decision 2008/615/JHA; Prüm Decision, 23.6.2008, Article 25(1).
[271] Treaty of Lisbon amending the TEU and the Treaty establishing the European Community, 2007.
[272] EU Declaration No 21 concerning the Charter of Fundamental Rights of the European Union, annexed to the Final Act of the Intergovernmental Conference which adopted the Treaty of Lisbon, 13.12.2007.
[273] TFEU, Article 16. See footnote 58.
[274] Fuster, 2014, p. 233. About the Charter, see Chapter 1.2.1.2.
[275] EU Council Act 2000/C 197/01, 29.5.2000.

2008/977/JHA[276], which applied only to data processing which had a cross-border dimension between the EU member states.

The DPD obliges the EU Commission to report to the Council and the Parliament on the Data Protection Directive´s implementation and propose for amendments, if necessary.[277] The Commission´s Communication of 2003, which reviewed the status of implementation of the DPD for the first time, stated that no legislative changes were necessary. The situation needed improvement and the Commission´s report contained a Work Programme for better implementation of the DPD.[278] In 2007 the Commission issued a new Communication and still it did not consider it necessary to amend the DPD.[279] This was before the signing of the Lisbon Treaty in 2007, after which the Commission´s opinion changed. In 2009 the Commission published a new consultation with a section on the protection of personal data and privacy, where it argued that the EU had to respond to the challenge posed by the increasing exchange of personal data and the need to protect privacy. The Commission referred to the Charter´s rights to privacy and the protection of personal data, and suggested that legislative initiatives may be necessary.[280]

The Council requested in 2009 that the Commission evaluates the functioning of EU instruments on data protection and if necessary to present legislative and non-legislative initiatives. The Council continued that the impact these will have on the rights to privacy and the protection of personal data should be recognized.[281] The Parliament welcomed a broad data protection system and invited the revision of the Council Framework Decision 2008/977/JHA. It asked the Commission and the member states to make sure that future EU action respects the fundamental rights and *"strikes the right balance between security and freedom, and that this objective is adequately monitored and streamlined"*.[282] The

[276] EU Council Framework Decision 2008/977/JHA, 27.11.2008.
[277] EU Data Protection Directive 95/46/EC, Article 33.
[278] EU Commission, First report on the implementation of the Data Protection Directive 95/46/EC. COM 265 final, 15.5.2003, p. 23.
[279] EU Commission, Communication from the Commission to the European Parliament and the Council on the follow-up of the Work Programme for better implementation of the Data Protection Directive, COM 87 Final, 7.3.2007.
[280] EU Commission, Communication from the Commission to the European Parliament and the Council— Area of Freedom, Security and Justice serving the citizen. COM 262 Final, 10.6.2009, p. 7-8.
[281] The Stockholm Programme (2010/C 115/01), an open and secure Europe serving and protecting citizens, OJ C 115, 4.5.2010, p. 1 and Chapter 3.4.2.
[282] EU Parliament, Resolution on the Communication from the Commission to the European Parliament and the Council – An area of freedom, security and justice serving the citizen – Stockholm programme, 25.11.2009, para 117.

Commission implemented the Council´s request into its Action Plan which stressed the importance of privacy in a global society where the data flows over borders. The EU´s approach must be strengthened in protecting the personal data in the context of all EU policies, including law enforcement. It is the Union´s task to ensure that the right to data protection is consistently applied.[283] In 2010 the Commission published its aim to propose a revision of the legal framework for data protection in 2011.[284]

3.1.2 Preliminary work at the EU institutions to protect the privacy

This chapter will explain how the protection of the right to privacy was written into the Data Protection Directive on Police Matters. The Commission published a legislative package in 2012, which consisted of a proposal for a Regulation on the protection of individuals regarding the processing of personal data and on the free movement of such data[285] - the GDPR to replace the DPD. There was also a proposal for a Directive on the protection of individuals regarding the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data[286] - the Data Protection Directive on Police Matters to replace the Council Framework Decision 2008/977/JHA.

The Commission accompanied these proposals with a Communication to safeguard privacy and advance the protection of personal data with ensuring that individuals have the right to enjoy control over their personal data.[287] The Communication contained the same innovations as its proposals, for an example the introduction of a right to be forgotten; the use of technologies to protect the privacy of information, default settings which are privacy-friendly and certification schemes for privacy; an obligation to notify of data breaches and to appoint data protection officers; the introduction of the privacy by design principle and the obligation to carry out data protection impact assessments; and the transformation of the Article 29 Working Party into the European Data Protection

[283] EU Commission, Action Plan Implementing the Stockholm Programme, 20.4.2010, Chapter 2.
[284] EU Commission, Communication to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions: A comprehensive approach on personal Data Protection in the European Union. COM 609 final, 4.11.2010, p. 18.
[285] EU Commission Proposal for a General Data Protection Regulation, COM(2012) 11 final, 25.1.2012.
[286] EU Commission Proposal for a Data Protection Directive on Police matters, COM 10 final, 25.1.2012.
[287] EU Commission, Communication: Safeguarding privacy in a connected world: A European Data Protection framework for the 21st Century. COM (2012) 9 final, 25.1.2012, p. 2.

Board.[288] Even though the term 'privacy' is mentioned in the Communication´s title and in the text, it does not appear in the proposals themselves.

The proposals for the GDPR and the Directive are based on the TFEU Article 16(2)[289], and then centered on the right to the protection of personal data. They both state that their objective is to protect the natural persons´ fundamental rights and freedoms and particularly their right to the protection of personal data.[290] The proposed legislation displaced privacy by personal data protection and it does not refer to Convention 108 which does have "privacy" in its text. The GDPR seems to hesitate between competing conceptions of what constitutes a limitation on the fundamental right to personal data protection. It resembles the wording of the ECHR Article 8(2) and of the Charter Article 52(1) when ruling on restrictions to the rules of the proposed GDPR, and when justifying the processing of personal data.[291] The idea of data protection law serving especially the right to privacy has been replaced with the claim that it develops the right to the protection of personal data. This right is not mentioned as connected with the right to privacy or as an element of it, but in place of it. It seems like the processing of personal data alone amounted to a limitation of the fundamental right to the protection of personal data.[292]

The proposed GDPR refers to "privacy" in the Recital dealing with sensitive data.[293] The GDPR states that the communication of data breaches to the data subjects is likely to harmfully affect the protection of the personal data or privacy of the data subject[294]. These are defined in the GDPR´s preamble as breaches that could result in identity theft or fraud, physical harm, significant humiliation, or damage to reputation[295].

The EPDS commented on the data protection reform and the proposal of the Data Protection Directive on Police Matters. It stated that data protection is closely related to the

[288] EU Commission, Communication: Safeguarding privacy in a connected world: A European Data Protection framework for the 21st Century. COM (2012) 9 final, 25.1.2012, p. 6-7, 9 & 11.
[289] TFEU, Article 16(2): see footnote 58.
[290] EU Commission Proposal for a General Data Protection Regulation, COM(2012) 11 final, 25.1.2012, p. 40, Article 1, and EU Commission Proposal for a Data Protection Directive on Police matters, COM 10 final, 25.1.2012, p. 27. Article 1.
[291] EU Regulation 2016/679, General Data Protection Regulation, Article 6 about lawfulness of processing and Article 22 about automated individual decision-making, including profiling.
[292] Fuster, 2014, p. 243-244.
[293] EU Commission Proposal for a General Data Protection Regulation, COM(2012) 11 final, 25.1.2012, Recital 41.
[294] EU Commission Proposal for a General Data Protection Regulation, COM(2012) 11 final, 25.1.2012, Article 32(1).
[295] Ibid, Recital 67.

fundamental value of the right to privacy. The Directive respects the legal obligations as stated in international and EU law, as well as recognizes that privacy and data protection are fundamental values for society and its´ individuals. The EDPS stated that specific rules are needed due to the specific nature of the police and justice sectors. Data protection in these sectors should be coherent with the general rules written in the proposed GDPR[296] and be specified only if necessary. According to the EDPS, the Council changed the Directive´s nature to provide minimum harmonization and the member states may offer higher safeguards for data protection. Different levels of protection standards in the Union will make the exchange of information more difficult and hinder the cooperation between the competent authorities.[297]

The EDPS refers to TFEU Article 16 which states that the Union must take care of the high standards of data protection and it cannot leave it to the member states alone.[298] The EDPS sees that the new Directive does not harmonize the field as much as the GDPR would if it also contained the field covered by the Directive, and that the Directive leaves too much room for interpretation to the member states of its rules.[299] The EDPS recommended the following sentence to the Directive´s Recitals: "*The processing of personal data should be designed to serve man... it should respect [natural person´s]… rights to privacy and the protection of personal data and contribute to the well-being of individuals… [and] to the accomplishment of an area of freedom, security and justice*"[300], but it did not get through.

The right to respect for private and family life is mentioned in the proposed Directive as one of the Charter´s rights that it respects "notably".[301] The word "privacy" is not in the final text, but the Directive claims to be respecting the Charter´s fundamental rights: the right to respect for private and family life and the right to the protection of personal data[302]. Through the reform the Commission aimed to improve the internal market dimension of data protection, improve the individuals´ exercise of data protection rights and to cover all areas of Union competence. It aims to ensure that individuals are in control of their personal data and that they feel they are being protected when their data is

[296] EU Regulation 2016/679, General Data Protection Regulation.
[297] European Data Protection Supervisor Opinion 6/2015, 28.10.2015, p. 4-5.
[298] TFEU, Article 16(1). See footnote 58.
[299] European Data Protection Supervisor Opinion 6/2015, 28.10.2015, p. 4-5.
[300] Ibid, Annex to the opinion, p. 5.
[301] EU Commission Proposal for a Data Protection Directive on Police matters, COM 10 final, 25.1.2012. P. 25.
[302] EU Data Protection Directive on Police Matters 2016/680, Recital 104.

processed.[303] This aim is a good goal but it is not sure yet, if the safeguards in the new Directive can reach it in practice. The GDPR and the Directive will step into use in 2018.

For the Union to be able adopt the Data Protection Directive on Police Matters it should be in accordance with the principles of subsidiarity and proportionality. The Union may adopt measures in accordance with the principle of subsidiarity as set out in the TEU Article 5[304]. The EU institutions acts must be appropriate for attaining the pursued legitimate objectives and do not exceed the limits of what is necessary and appropriate to achieve those objectives.[305] The principle establishes two tests: the test of suitability and the test of necessity. The first measures whether the mean being used is suitable to reach the pursued ends. The second measures the competing interests: the consequences of restrictions, the right to legal protection, and if the consequences can be justified.[306] The new Directive does not go beyond the principle of proportionality. The Directive´s objectives (the protection of the natural persons´ fundamental rights and freedoms and their right to the protection of personal data and to ensure the free exchange of that data by competent authorities within the EU) can be more sufficiently achieved at the Union level.[307]

3.2 The Data Protection Directive on police matters

This chapter will introduce the Data Protection Directive on Police Matters. The Directive is quite long as it contains 107 Recitals and 65 Articles, so it does not serve this thesis to go through them all one by one. Instead the introduction will be based on the rules it

[303] EU Commission Impact Assessment, SEC(2012) 72 final, 25.1.2012, Chapter 4, and p. 41.
[304] TEU Article 5: "*1. The limits of Union competences are governed by the principle of conferral. The use of Union competences is governed by the principles of subsidiarity and proportionality. 2. Under the principle of conferral, the Union shall act only within the limits of the competences conferred upon it by the Member States in the Treaties to attain the objectives set out therein. Competences not conferred upon the Union in the Treaties remain with the Member States. 3. Under the principle of subsidiarity, in areas which do not fall within its exclusive competence, the Union shall act only if and in so far as the objectives of the proposed action cannot be sufficiently achieved by the Member States, either at central level or at regional and local level, but can rather, by reason of the scale or effects of the proposed action, be better achieved at Union level. The institutions of the Union shall apply the principle of subsidiarity as laid down in the Protocol on the application of the principles of subsidiarity and proportionality. National Parliaments ensure compliance with the principle of subsidiarity in accordance with the procedure set out in that Protocol. 4. Under the principle of proportionality, the content and form of Union action shall not exceed what is necessary to achieve the objectives of the Treaties. The institutions of the Union shall apply the principle of proportionality as laid down in the Protocol on the application of the principles of subsidiarity and proportionality*."
[305] CJEU, Joined cases C-92/09 and C-93/09, Schecke and Eifert, 9.11.2010, para 74.
[306] Barnard, 2013, p. 177.
[307] EU Data Protection Directive on Police Matters 2016/680, Recital 93.

directs to the member states to implement, which serve the protection of privacy when national public authorities process personal data.

The Data Protection Directive on Police Matters is for *"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*" including the prevention of threats to public security.[308] It repealed the Council Framework Decision 2008/977/JHA.[309] This Directive applies to the national competent authorities' processing of personal data by automated means for the above-mentioned purposes and to the processing of such data.[310] It seeks to uniform the protection of personal data and to facilitate the exchange of data between member states competent authorities. The point is to enable effective judicial cooperation in criminal matters, although it steps into the member states´ sovereignty.[311]

The Directive is divided into chapters based on their issues: general provisions; principles; rights of the data subject; controller and processor; transfers of personal data to third countries or international organizations; independent supervisory authorities; cooperation; remedies, liability and penalties; implementing acts; and, final provisions. The member states must adopt national legislation to comply with the Directive by 6.5.2018.[312]

3.2.1 The objectives of the new Directive

This chapter will introduce the objectives of the new Directive. The protection of personal data should be guaranteed equally everywhere in the EU. The Data Protection Directive on Police Matters serves to protect personal data in the work of the public authorities. It aims to ensure that the natural person´s level of protection of rights and freedoms is equivalent throughout the EU, in relation to the processing of their personal data by national public authorities.[313] Through the Directive, the EU institutions enable the personal data to flow freely between the national authorities, to prevent, investigate and prosecute crimes or

[308] Ibid, Name of the Directive and Article 1.
[309] EU Data Protection Directive on Police Matters 2016/680, Article 59.
[310] Ibid, Article 2.
[311] Oikeusministeriö, 12.10.2016, Chapter 3.
[312] EU Data Protection Directive on Police Matters 2016/680, Article 63(1).
[313] Ibid, Recital 7.

execute criminal penalties. The aim is also to prevent threats to public security and to transfer the personal data to third countries and international organizations. The high level of protection of personal data should be maintained in all this. The protection should not depend on the used techniques or of the authorities´ instruments. The Directive applies to natural persons, whatever their nationality or place of residence.[314]

The EU has adopted instruments in the field of judicial cooperation in criminal matters before adopting this new Directive. These specific provisions of acts should stay unaffected.[315] These are for example, the provisions in the Prüm Decision[316], or the Convention on Mutual Assistance in Criminal Matters between the Member States of the EU[317]. The Directive states in its Recitals that the Commission should evaluate the relationship between this Directive and those acts adopted before it. The Commission should evaluate the need for adjusting and if necessary to make proposals to create coherent legal rules of those provisions with this Directive.[318] This is to ensure that the protection of personal data is guaranteed equally everywhere in the EU

The GDPR[319] spells general rules to ensure the free movement of personal data and to protect natural persons in relation to the processing of personal data within the EU. The new Directive and the GDPR supplement each other as they operate in different sectors but cooperate in the areas where they overlap. As an example, the GDPR applies when a competent authority lawfully discloses personal data to a recipient who is not a competent authority defined by the Directive. When the competent authority has collected personal data for one of the Directive purposes, the GDPR applies when that data is processed for other purposes than the ones named in this Directive.[320]

3.2.2 The principles of the new Directive

The Data Protection Directive on Police Matters repeats the principles of the data protection law established already in the DPD[321]. The difference is, as already mentioned,

[314] Ibid, Recitals 4 & 17-18.
[315] Ibid, Article 61.
[316] EU Council Decision 2008/615/JHA; Prüm Decision, 23.6.2008.
[317] EU Council Act 2000/C 197/01, 29.5.2000.
[318] EU Data Protection Directive on Police Matters 2016/680, Recital 94.
[319] EU Regulation 2016/679, General Data Protection Regulation.
[320] EU Data Protection Directive on Police Matters 2016/680, Recital 34.
[321] EU Data Protection Directive 95/46/EC, Article 6.

that for the first time the Union directs these principles to apply also in the field of police matters. This chapter will go through the most relevant of these.

The processing of personal data must be lawful, fair and transparent and used for specific purposes mentioned in law. The purpose for 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.[322] The member states shall make sure that personal data is:[323]

- processed lawfully and fairly;
- collected for specified, explicit and legitimate purposes and not processed in a manner that is incompatible with those purposes;
- adequate, relevant and not excessive compared to the purposes why they are processed;
- accurate and kept up to date;
- kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which they are processed; and
- processed so that the data´s security is ensured, including protection against unauthorized or unlawful processing and against accidental loss or damage.

The data controller must prove he complies with the above set rules.[324] The stored personal data must be reviewed and erased periodically after appropriate time limits.[325] The concept of purpose 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.[326]

The right of presumption of innocence, as ordered by the Charter should not be threatened in the data processing especially when establishing different categories of data registries for natural persons. Different data subjects should be distinct from each other, such as persons suspected of committing a crime, persons convicted of a crime, and victims, and other parties such as witnesses.[327] 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. When personal data is sent to other authority, the

[322] EU Data Protection Directive on Police Matters 2016/680, Recital 26.
[323] Ibid, Article 4(1).
[324] Ibid, Article 4(4).
[325] Ibid, Article 5.
[326] Bräutigam, 2016, p. 161.
[327] EU Data Protection Directive on Police Matters 2016/680, Recital 31 & Article 6.

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.[328]

The data subject´s consent does not provide a legal basis for processing personal data by competent authorities. A national competent authority may process personal data if that is necessary for performing its tasks according to the objectives set in the Directive´s Article 1(1). These must also be based on member state law, which specifies the objectives of the processing, it´s purposes and the processed personal data.[329] The competent authorities may process personal data for other purposes than the ones´ set in the Article 1(1), if it fulfils the conditions of the Article 9[330]. Sensitive personal data can be processed if it is strictly necessary, with safeguards and where authorized by law to protect the natural person´s interests, or if the data subject has made the data public herself.[331] A decision which is based on automated processing and produces harmful effects to the data subject, should be authorized by the law of the data subject and provide appropriate safeguards for her.[332]

3.2.3 The rights of the data subject and obligations of the data controller

This chapter introduces the rights of the data subject and the obligations of the data controller. Data processing may risk individual´s rights and freedoms and it may result to

[328] Ibid, Article 7.
[329] Ibid, Recital 35, Article 8.
[330] Ibid, Article 9: "*1. Personal data collected by competent authorities for the purposes set out in Article 1(1) shall not be processed for purposes other than those set out in Article 1(1) unless such processing is authorised by Union or Member State law. Where personal data are processed for such other purposes, Regulation (EU) 2016/679 shall apply unless the processing is carried out in an activity which falls outside the scope of Union law. 2. Where competent authorities are entrusted by Member State law with the performance of tasks other than those performed for the purposes set out in Article 1(1), Regulation (EU) 2016/679 shall apply to processing for such purposes, including for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, unless the processing is carried out in an activity which falls outside the scope of Union law. 3. Member States shall, where Union or Member State law applicable to the transmitting competent authority provides specific conditions for processing, provide for the transmitting competent authority to inform the recipient of such personal data of those conditions and the requirement to comply with them. 4. Member States shall provide for the transmitting competent authority not to apply conditions pursuant to paragraph 3 to recipients in other Member States or to agencies, offices and bodies established pursuant to Chapters 4 and 5 of Title V of the TFEU other than those applicable to similar transmissions of data within the Member State of the transmitting competent authority*."
[331] Ibid, Article 10.
[332] Ibid, Article 11.

physical, material or non-material damage to the concerned person.[333] The new Directive has one chapter for the data subject´s rights. These rights contain rules of information that must be made available to the data subject, her right of access to her personal data and the provisions on limiting the right of access, the right to rectify or erase her data or to restrict the processing, and her rights in criminal proceedings. Also, the competent supervisory authority may exercise and verify the data subject´s rights.[334]

The limitations to the data subject´s rights of access set in the Directive Article 15 are going to be dealt in detail in the chapter 4.3. This is because the Article allows the member states to adopt measures which restrict the data subject´s right of access to her data, with one basis being to protect national security.

The member states shall establish the data controller's liability for processing personal data. The controller's activities have to comply with the new Directive and the controller must implement measures, which take into account the data protection principles by design and data protection by default, and evaluate the processing's purposes, context, scope and nature and the risk to the data subject´s rights.[335] The member states shall adopt laws which govern the processing by a processor and include a contract which binds the processor to the controller and require that the processor acts under the controller's instructions. The processing must be able to be monitored and the controller or processor must record its processing activities (a log containing at least the identification of the person who consulted or disclosed personal data and the justification for the processing[336]) and cooperate with the supervising authority.[337] The controller or processor has to evaluate the processing's risks and implement measures to reduce them, such as encryption, to

[333] Ibid, Recital 51. In particular: "*where the processing may give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of data protected by professional secrecy, unauthorized reversal of pseudonymisation or any other significant economic or social disadvantage; where data subjects might be deprived of their rights and freedoms or from exercising control over their personal data; where personal data are processed which reveal racial or ethnic origin, political opinions, religion or philosophical beliefs or trade union membership; where genetic data or biometric data are processed in order to uniquely identify a person or where data concerning health or data concerning sex life and sexual orientation or criminal convictions and offences or related security measures are processed; where personal aspects are evaluated, in particular analyzing and predicting aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behavior, location or movements, in order to create or use personal profiles; where personal data of vulnerable natural persons, in particular children, are processed; or where processing involves a large amount of personal data and affects a large number of data subjects*."
[334] Ibid, Articles 12 - 18.
[335] Ibid, Recitals 50, 52 & 53, Articles 19 - 20.
[336] Ibid, Recitals 55 & 57.
[337] Ibid, Articles 21 - 28.

maintain security and to prevent processing that is against this Directive. In case personal data is infringed, the controller notifies the supervisory authority unless the breach does not risk the person´s rights. In case of a risk, the data subject should be notified of it and guided on how to minimize further damages.[338] EU law has no specific rule to ensure that the uses of encryption and anonymization techniques are protected.[339]

The national supervisory authority monitors the application of this Directive to protect natural persons regarding the processing of their personal data. The concept of supervisory authority was already introduced in the chapter 1.1 in relation to Convention 108 and the CoE Police Recommendation. The Data Protection Directive on Police Matters demands the member states to establish an independent supervisory authority. The supervisory authority (or several, each with a separate task, adequate resources, and public annual budget) monitors the application of the rules adopted based on this Directive. Member states have already established the supervisory authority under the GDPR and the tasks under the new Directive may be transferred to this authority.[340] The supervisory authority handles the data subjects' complaints and investigates the matter, or transmits it to the competent authority, and then it informs the data subject of the progress and the outcome. The authorities' tasks and powers to perform should be equal in each member state. They should be able to bring the Directive´s violations to the attention of the judicial authorities or to engage in legal proceedings. The supervisory authorities in different member states cooperate with each other and with the Commission.[341]

Member states must implement and impose penalties, which are effective, proportionate and deterrent, on persons who breach the Directive. If data subject considers that her rights under this Directive are breached or if the supervisory authority does not act on her complaint, she has the right to have an effective judicial remedy in accordance with the Charter Article 47[342]. She has the right to a remedy at the national court where the

[338] Ibid, Recitals 60 - 62 and Articles 29 - 31.
[339] Cocq, 2016, p. 190.
[340] EU Data Protection Directive on Police Matters 2016/680, Recitals 75-77, Article 41.
[341] Ibid, Recital 81-83, Articles 45 - 47.
[342] Charter of fundamental rights of the EU, 2009, Article 47: "*Right to an effective remedy and to a fair trial. Everyone whose rights and freedoms guaranteed by the law of the Union are violated has the right to an effective remedy before a tribunal in compliance with the conditions laid down in this Article. Everyone is entitled to a fair and public hearing within a reasonable time by an independent and impartial tribunal previously established by law. Everyone shall have the possibility of being advised, defended and represented. Legal aid shall be made available to those who lack sufficient resources in so far as such aid is necessary to ensure effective access to justice.*"

supervisory authority is established, against that authority´s decision producing legal effects concerning her.[343]

3.2.4 Data protection and exchange of information in relation to third countries

The EU member state´s public authorities may transfer information to other states´ public authorities in relation to their work. So far this has been regulated by Convention 108, guided by the CoE Police Data Recommendation[344] and the Council Framework Decision 2008/977/JHA. The Data Protection Directive on Police Matters states that a member state´s competent authority can send personal data to a third country´s competent authority, if the transfer fulfils the conditions of the Directive. These conditions being that the transfer is necessary, the receiving authority is authorized by this Directive and the third country ensures an adequate level of protection.[345] The member states must make sure when public authorities transfer personal data to a third country, that it takes place only if it is necessary to prevent, investigate or prosecute crimes or to execute convictions. This includes the prevention of threats to public security and that the recipient´s data controller fulfils the Directive´s definition of a competent authority. Only the competent authorities acting as controllers should carry out the transfers.[346]

When personal data is sent over the national borders, it may endanger the data subject´s possibility to exercise her data protection rights, and the supervisory authorities may become unable to operate outside their borders. The cooperation between the supervisory authorities needs development to help them exchange information with their foreign counterparts. The Data Protection Directive on Police Matters also recognizes this[347].

In relation to data exchange from the EU to third countries, the EU Commission´s main role is to ensure that the data protection principles are recognized. The Commission decides for the whole EU that third countries and international organizations provide an adequate level of protection. This is to reach EU wide uniformity and legal certainty. The definition for the adequacy of the protection was derived from the CJEU´s interpretation in

[343] EU Data Protection Directive on Police Matters 2016/680, Recital 86-87, Articles 52 - 57.
[344] CoE Police Data Recommendation Rec(87)15, 17.9.1987.
[345] EU Data Protection Directive on Police Matters 2016/680, Articles 35 - 36(1).
[346] Ibid, Recital 64, Article 37 - 38.
[347] Ibid, Recital 74, Article 40.

the *Schrems* case[348] and from there written to the recitals of this Directive.[349] The level of protection in a third country is adequate when it is essentially equivalent to that in the EU. The "essentially equal" standard is hard to meet in the field of national security law. Its assessment should be reflecting reality, not just the ideal world of law as written in the books. The doings of European authorities are not always transparent either. In 2016, the German secret service was excessively collecting data and spying on EU partners and NATO.[350]

The Commission observes how the third country respects the rule of law, access to justice and the international human rights standards, as well as recognizes the third country´s participation in multilateral systems and the implementation of their obligations, as an example the accession to Convention 108. It looks at the legislation concerning national security, public order and criminal law. The Commission consults with the EDPB[351] when evaluating the protection in third countries or international organizations. It should also consider its previous decisions adopted in accordance with the GDPR Article 45.[352] The Commission prohibits the data transfers to that recipient which no longer provides an adequate level of protection. The transfers are again allowed if adequate safeguards are provided in a legally binding instrument (such as bilateral agreement).[353] The Directive´s implementing powers are given to the Commission. This is to uniform the conditions for the implementation regarding the adequate level of protection provided by a third country and the cooperation between the supervisory authorities and the EDPB. If a third country no longer provides adequate protection, the Commission can adopt immediately applicable acts.[354]

3.3 Conclusion of the section 3

This section introduced the EU´s data protection reform and the coming changes of the legislation on data protection in police matters. The reform is necessary as the EU is

[348] CJEU, C-362/14, Schrems, 6.10.2015.
[349] EU Data Protection Directive on Police Matters 2016/680, Recital 67.
[350] Bräutigam, 2016, p. 168.
[351] European Data Protection Supervisor (EDPS), Overview. European Union, online: https://europa.eu/european-union/about-eu/institutions-bodies/european-data-protection-supervisor_en, 20.8.2016. Ensures that EU institutions respect people's right to privacy when processing their personal data.
[352] EU Data Protection Directive on Police Matters 2016/680, Recital 66 - 68.
[353] Ibid, Recital 69 - 71.
[354] Ibid, Recitals 90 & 92 and Article 36(5).

responding to the challenge posed by the increasing exchange of personal data and the need to ensure the rights to data protection and the privacy in all EU competences. It is the Union´s task to ensure that the right to data protection is consistently applied. Thus the GDPR and the Data Protection Directive on Police Matters have been adopted by the EU and they both will come into force in 2018.

This section also explained how the national authorities' rights to process personal data are changing and what steps were taken in the process. The introduction of the Data Protection Directive on Police Matters covered the instrument´s main objectives and principles for data processing; the rights of the data subject and the obligations of the data controller and the national supervisory authorities; and the protection of personal data when it is transmitted to third countries.

The Directive is abstract and needs clarification. It uniforms the member states data protection legislation in the field of police matters by setting the minimum level of harmonization. The Directive uses the phrase "shall provide", when it directs the member states to implement rules. This is partly a result of compromises between the member states respective interests. This issue of abstractness will be discussed in the section 4.

4 THE DATA PROTECTION DIRECTIVE ON POLICE MATTERS PROTECTS PRIVACY

This section introduces the current national legislation dealing with data protection in the national public authorities work by using the Finnish legislation as an example of a member state´s law. The member states may face problems when implementing the Data Protection Directive on Police Matters, but as the implementation process has only begun it is difficult to say what is going to change in the national legislations. Finally, this section lays out possible advantages and problems of the uniform data protection legislation on police matters in the EU. Uniformity ensures equal protection and improves cooperation between the authorities, but the abstract new Directive allows the member states to adopt national legislations which differ significantly from each other.

4.1 It is important to protect the privacy in the data protection legislation

When a fundamental right collides with a collective good, it requires balancing and proportionality to define the right legal outcome. Balancing is necessary when laws are applied by an authority because fundamental rights provisions are vague.[355] At his New Year´s speech in 2017, Finland´s President Mr. Sauli Niinistö addressed the balancing of the individuals´ fundamental rights and the authorities´ rights to gather data. He stated that the Finnish Constitution protects individual´s rights but we are facing questions, such as how should we react when we are balancing the collective security and the individual´s rights. When something bad happens, someone will ask why we did not do enough to stop the terrorism. And a bad answer is that we did not have sufficient powers. "*A key role is played by effective data gathering and exchange of information and flexible co-operation between the authorities of different countries. Action is needed from the EU*".[356]

Before 2000, the right to respect for private life was often seen as including the protection of personal data as its´ informational dimension.[357] This approach was then replaced by the idea that these were two separate notions: the protection of the respect for private life and the protection of personal data. They are closely related and overlap in some cases. The protection of personal data was part of a wider respect for privacy, but at the same time it was also different from it. The right to protection of personal data can be explained as

[355] Vainio, 2016, p. 251.
[356] New Year Speech by President of the Republic Sauli Niinistö, 1.1.2017.
[357] Benyekhlef, 1996, p. 91.

resulting from a widening of the right to privacy, but being autonomous.[358] The protection of personal data is especially important for the right to privacy.[359] It may be difficult to separate these two rights, the right to data protection and the right to privacy. Some find these two to be one; some find that the protection of personal data adds to the protection of privacy; and some consider these to be two separate rights but connected to each other. As an example, in the data protection reform process, the German Government claimed to find it difficult to draw the line between the right to privacy and the right to data protection because in Germany the right to data protection is derived from the right to privacy. For another example, the Swedish Government found it difficult to understand clearly the concept of individual´s right to control her own data.[360]

The CJEU stated in December 2016 that the right to the protection of personal data of the Charter Article 8 concerns a fundamental right which is distinct from that enshrined in the Charter Article 7 (the right to respect of private life) and which has no equivalent in the ECHR. The Court refused to state whether the protection guaranteed by the Charter Articles 7 and 8 is wider than that guaranteed in the ECHR Article 8.[361]

The EDPS stated in its opinion of the proposed Directive, that data protection is closely related to the fundamental value of the right to privacy, and the CJEU confirms the importance of a protection in connection with law enforcement and national security. The CJEU warned in the case *Digital Rights Ireland* that data retention by authorities is "*likely to generate in the minds of the persons concerned the feeling that their private lives are the subject of constant surveillance*"[362], and in the *Schrems* case the CJEU considered that public authorities access to the content of electronic communications affects the essence of the right to privacy if it is enabled on a generalized basis.[363] The problem is how much freedom for data processing can the legislator give to the public authority for the investigative work without compromising the essence of the data subjects´ privacy. In 1984 Judge Pettiti explained in his concurring opinion to the judgement of the ECtHR case *Malone v. UK*, that the CoE´s mission is to prevent the systems that would allow "Big

[358] Fuster, 2014, p. 214.
[359] CJEU, Joined cases C-293/12 and C-594/12, Digital Rights Ireland, 8.4.2014, para 53.
[360] Fuster, 2014, p. 92.
[361] CJEU, Joined cases C-203/15 and C-698/15, Tele2 Sverige AB, 21.12.2016, para 129 & 131. About the Charter, see Chapter 1.2.1.2.
[362] CJEU, Joined cases C-293/12 and C-594/12, Digital Rights Ireland, 8.4.2014, para 37.
[363] CJEU, C-362/14, Schrems, 6.10.2015, para. 94.

Brother" to become master of the citizen's private life. It is just as serious to be made subject to measures of interference against one's will as to be unable to stop such measures when they are illegal or unjustified.[364] Mrs. Viviane Reding, the Vice-President of the Commission, stated in the EU Parliament in a debate concerning the forthcoming Directive, that the freedom and security of citizens are two sides of the same coin. They are two policy objectives that should be pursued in parallel. One cannot advance without the other, and one should not eliminate the other.[365] The Directive respects the fundamental rights recognized in the Charter.[366]

The CJEU cases *Digital Rights Ireland*[367] and the *Schrems*[368] increased commenting on the issue in the media. One comment after the *Digital Rights Ireland* decision sums up the result after these decisions: "*More of these types of initiatives are needed in order to assure effective privacy and data protection*"[369]. Most member state's constitutional courts follow the reading of the *Digital Rights Ireland* judgment and are in line with the CJEU's reasoning.[370] Because of the CJEU´s rulings, several states´ courts invalidated their data retention legislation (i.e. Netherlands and Belgium), and some states amended their legislation (i.e. UK and Luxembourg).[371] But many Governments interpret that the fundamental rights do not have the same weight, and that interception of communication data is a powerful tool to protect state security. The Finnish Constitutional Law Committee stated that there is no obstacle to the retention of data, if the proportionality requirements are met in other ways. The Finnish government is preparing surveillance legislation that would allow authorities' search-term based access to internet data.[372] These CJEU rulings should impact the upcoming law and make it difficult to adopt if it is like those national laws which are now being amended around EU. The current Constitution does not allow the limitation of the right to privacy on basis of precautionary security. The constitution needs amending.[373]

[364] ECtHR, No. 8691/79, Malone v. UK, 2.8.1984, Judge Pettiti, concurring opinion.
[365] EU Parliament Debates, 11.3.2014.
[366] EU Data Protection Directive on Police Matters 2016/680, Recital 104; Charter of fundamental rights of the EU, 2009, Articles 7 and 8. See Chapter 1.2.1.2.
[367] CJEU, Joined cases C-293/12 and C-594/12, Digital Rights Ireland, 8.4.2014, para 23.
[368] CJEU, C-362/14, Schrems, 6.10.2015.
[369] Lynskey, 2014.
[370] Vainio, 2016, p. 233.
[371] Franssen, 2016.
[372] Vainio, 2016, p. 242 & 251.
[373] Sajari, 2016.

4.2 Member states´ national legislation in the field currently

The law which is still covering data protection in the work of the national investigative authorities will be in force until May of 2018 when the Data Protection Directive on Police Matters enters force. Before the upcoming Directive the EU member states had the possibility to independently interpret the principles of protection of personal data processed in the framework of police cooperation in criminal matters as set in Convention 108. When the national authorities transmit personal data to other states' authorities, it is covered by the Council Framework Decision 2008/977/JHA[374] if that member state has implemented the Decision into its national law.

This paper shall use the Finnish national law as an example of the member state's national legislation covering the field. It is not necessary to go through the law with the same accuracy as the data protection law in EU, as the Inspector general, at the Office of the Finnish Data Protection Ombudsman, Mr. Heikki Huhtiniemi says that the Finnish law covering the police work has already implemented the data protection principles of the Data Protection Directive and the Council Framework Decision 2008/977/JHA.[375] EU law did not require this, but the Finnish legislator was willing to.

4.2.1 What the Finnish authorities may do with the possessed personal data

These principles guide all data processing in Finnish police work: the processing of personal data is based on law and in the course of lawful duty of the police, personal data is processed transparently, and the quality of the data and the rights of the registered person are guaranteed.[376] If a Finnish police officer wants to check someone’s personal data from the authority’s data systems, the right to do so has to be granted by a specific national law. In Finland, the Data Protection Code[377] and the National Police Act[378] states that the officer has to have a special work related purpose for exercising her authority, or that the utilization of the data is necessary to ensure state security, to prevent a threat to life, or to

[374] EU Council Framework Decision 2008/977/JHA, 27.11.2008.
[375] Huhtiniemi, 2016.
[376] Poliisihallitus, 2010.
[377] Finnish Personal Data Code, Henkilötietolaki 523/1999, specifically Chapter 1 Article 7: (limitation for specific purpose) and Section 8: (General precondition for processing).
[378] Finnish Police Code, Poliisilaki 872/2011, Chapter 1 Section 5: (principle for limited purpose).

prevent or investigate an offence subject to imprisonment.[379] The Finnish Act on the Processing of Personal Data by the Police (Laki henkilötietojen käsittelystä poliisitoimessa 761/2003) applies to the processing of personal data needed for the performance of police duties. Firstly, this Act lists different police information systems used in Finland. Then it sets special provisions on processing personal data, and utilizing and supplying that data e.g. for purposes of their collection and the other purposes. After these it has provisions for deleting and archiving data, then provisions on processing personal data in connection with international police cooperation. After these come the rights of data subjects.[380]

A landmark judgement on data protection issued in Finland by the Finnish district Courts came in 2014, when 72 police officers were convicted for data protection offences[381] and for violating their official duty[382]. They had been scanning sensitive personal information of a famous cross-country skier Mr. Mika Myllylä. The convicted officers had been curious about the Olympic medalist´s cause of death in 2011 and they had no special work related purpose for checking his files.[383]

The Finnish Code for police registries´ sets the rules for the police when it is exchanging data with foreign countries.[384] The police have the right to give personal data from the police files to the International Criminal Police Organization or to its member states´ officials whose task is to maintain order in the society or crime prevention, investigation and prosecution.[385] It may also supply data to foreign police authorities, or to other

[379] Laki henkilötietojen käsittelystä poliisitoimessa 761/2003, Section 16.
[380] Ibid, Section 1, and Chapters 2 - 8.
[381] Rikoslaki 39/1889, Finnish Criminal Code, Chapter 38, Section 9, Henkilörekisteririkos.
[382] Ibid, Chapter 40 Section 9, Virkavelvollisuuden rikkominen.
[383] Reinboth, 2014.
[384] Laki poliisin henkilörekistereistä 509/1995, Chapter 5 Section 20.
[385] Ibid, Section 17(1-3): *The police has the right to transfer information from the personal data file to another police department or police staff whose purpose is to carry out the tasks referred to in the Police Code 1(1), if it is necessary to carry out these tasks. However the information referred to in Section 10 shall be made only when it is necessary to: 1) To ensure the national security; 2) Prevent an immediate threat to life or health, or significant damage to property; or 3) Prevent or investigate an offence which may result into imprisonment. Police department and police officer has the right to transfer information to another police department or police officer from a personal data file set up to carry out the tasks referred to in the Police Code 1(2) if it is necessary to carry out the task, for which the data is collected and stored*. and (Laki poliisin henkilörekistereistä 509/1995) Section 18(1-3): *Exchange of information to the police for any other purpose. In addition to what the Section 17 of the Code provides a police department and a police officer has the right to exchange the police register information to another police department or an officer if the information is necessary:1) To ensure national security;2) To prevent an immediate threat to life or health, or significant damage to property; or3) To prevent or investigate an offence which may result into imprisonment;4) To establish the identity of a person when performing a specific police duty which requires the verification of the identity; or 5) To decide or administer an opinion for issuing a license or its validity, if the precondition for issuing or the validity of the authorization is the license applicants or license holders*

authorities in such states whose duties include securing judicial and social order, maintaining public order and security, or preventing or investigating offences and forwarding them to a prosecutor. The data may be supplied if it is essential to ensure state security, prevent a danger threatening life or health or to prevent significant damage to property, or prevent or investigate an offence subject to imprisonment.[386]

Investigative authorities have to be able to process personal data beyond the context when collected for the prevention, investigation, detection or prosecution of specific criminal offences in order to understand criminal activities and to link different crimes. But the processing has to be connected to detective work, it must be for a particular and a legal purpose and it must be proportionate. As the professionals say – detectives should know what´s going on in their district. This need is also recognized in the new Directive.[387]

4.2.2 Data protection rules applied in practice

This chapter introduces how the data protection principles are implemented and applied in practice in the work of the national public authorities. When asked about the level of data protection in other EU member states, Mr. Huhtiniemi considered himself being unable to answer. It would require research on how protection is ensured in practice, although this would not only be done by looking at the provisions of the law.[388] There are differences between the 28 member states. One concrete example of the differences between the legislation of the member states can be found in the ECtHR case *S. And Marper v. UK*, which showed the different approaches of the CoE member states on compulsory taking of DNA information in the context of criminal proceedings. In some countries, it was limited to only specific circumstances, however in the UK, it was systematic and indefinite retention, irrespective of the suspected offence or the age of the offender.[389]

In 2013 the CoE published a report[390] on how the CoE member states have implemented the CoE Police Data Recommendation[391] rules in their national legislations (25 years after

---

reliability, suitability or other such condition, whose assessment requires data related to the license applicants or license holder's state of health, substance abuse, a committed crimes or to violent behavior.
[386] Laki henkilötietojen käsittelystä poliisitoimessa 761/2003, Section 40.
[387] EU Data Protection Directive on Police Matters 2016/680, Recitals 27 & 29.
[388] Huhtiniemi, 2016.
[389] ECtHR, No. 30562/04 and 30566/04, S. and Marper v. UK, 4.12.2008, paras 45-47.
[390] Prof. Cannataci & Dr. Caruana, 2013.
[391] CoE Police Data Recommendation Rec(87)15, 17.9.1987.

adopting the Recommendation). This research was done by sending questionnaires to the national authorities of the member states. The respondents were often unable to provide information on how the data protection law is applied in practice. The results showed clear differences in the provided level of protection in the member states. The fact that the CoE states claim to have implemented the rules of Convention 108 does not mean that those standards are achieved or that they would be high enough.[392] This supports the recognition of the Union institutions of the need to issue a reform package adopting two instruments - the GDPR and the Directive - to make the protection uniform in the EU. The EU does not have similar research of the Council Framework Decision 2008/977/JHA.

In Finland, in addition to the national law, the National Police Board and the Ministry of the Interior have granted approximately over one hundred different manuals, handbooks and orders to instruct the police work. In practice these manuals guide the officer´s everyday work. Each action the authorities do has its own set of rules. For example, there is a binding order covering the registration of data to the police data system[393], and an order for utilization of the police data in official duty[394]. Finnish police provide practical information to everyone on how her personal information is processed. This information is generally available at the official police web-site (www.poliisi.fi) and in every police station´s customer service desk (to mention two). The police´s customer can find information from the police documents of the issue in question and the officers are supposed to inform and guide the customer about her rights in the situation at hand.[395]

The rules on how to handle classified information can be mentioned as an example of those specific manuals guiding the work. If taken literally, police officer is not allowed to leave any papers containing classified information (e.g. sensitive personal data) on her desk when leaving her office even if the room can be locked. Such documents must be in a locked shelf and the classified information with the highest rating may be stored only in vaults, etc. Officers are not allowed to send classified information via normal e-mail, but via secured e-mail. Every paper (documents and notes) containing classified information,

[392] Prof. Cannataci & Dr. Caruana, 2013, p. 49.
[393] Ohje tietojen kirjaaminen poliisiasiain tietojärjestelmään (PATJA) 2020/2013/5231, 17.12.2013.
[394] Ohje poliisin tietojen käytöstä virkatehtävissä POL-2016-4458, 18.04.2016.
[395] Henkilötietolaki 523/1999, Section 24; Laki henkilötietojen käsittelystä poliisitoimessa 761/2003, Section 43; Laki viranomaisten toiminnan julkisuudesta 621/1999, Section 18.

which becomes useless, must be fully destroyed via specific secured system as they are not allowed to be left in a form or in a place, where outsiders can get a hold of them.[396]

These manuals are available to every officer in the police online system called Sinetti, but perhaps due to the vast amount of these handbooks and continuously changing regulations, they are not circulated among the officers when published or amended. In practice, it is impossible for every officer to know and apply these orders and manuals and it is crucial to know how personal data and privacy are protected in practice.

Every Finnish police officer goes through a three and a half year long professional education, which also covers data protection matters, before the officer can begin using the police data systems.[397] When in actual work, every officer must pass a compulsory online course and an examination covering the police personal data law to be allowed to process personal data in her work (in Finnish: Poliisin henkilötietolaki -verkkokurssi). This course goes through the most important provisions covering the processing of personal data in everyday police work. These include practical examples from the work which concerns the manuals and handbooks granted by the National Police Board. The course covers the relevant definitions, general principles of processing data, the purpose limitation of the processing, the data subject´s rights and access to her data, different data systems and their usage, security matters, DNA and fingerprint gathering, etc.[398] The course consists of three pre-exams and a final exam. Then another online course handles the police data systems covering the aspects of use of those systems and their maintenance, controlling data security problems and the usage of the secured e-mail in the police work.[399]

Currently most of the Finnish police officers investigate crimes by using papers and producing more papers (questioning forms, crime reports, etc.). When the criminal investigation is ready, the practice is that the police then store one copy of the report to a vault and send two paper copies to the public prosecutor and one copy to each party of the

[396] Määräys Poliisin salassa pidettävien tietoaineistojen käsittely POL-2015-3101, 3.6.2015, p. 15-17.
[397] Poliisiammattikorkeakoulu, 2016.
[398] See for example the Perustuslaki 731/1999, Henkilötietolaki 523/1999, Laki henkilötietojen käsittelystä poliisitoimessa 761/2003, Määräys rekisterinpito poliisissa 2020/2011/1423, 26.5.2011, and Ohje rekisteröidyn oikeuksien toteuttaminen poliisissa: tarkastusoikeus, tiedon korjaaminen ja informointi 2020/2012/66, 23.1.2012.
[399] Määräys poliisin tietojärjestelmien käyttö ja ylläpito 2020/2012/1302, 13.2.2013, Määräys tietoturvahäiriöiden hallinta poliisissa 2020/2012/1303, 13.2.2012, Määräys sähköpostin käyttöperiaatteet sisäaisianministeriön hallinnonalalla SMDno/2012/806, 11.2.2013.

investigation. In simple, a normal crime with one victim and one offender produces at least five piles of paper. One practical example of a safer way to handle personal data in a criminal investigation is to process everything electronically in the police data systems, instead of storing them as papers in folders. This way the documents are always behind at least one password. The practice of sending two paper copies of the report to the prosecutor is based only on internal procedure, not law. This automated processing of reports is not yet common in Finnish police work, but it is slowly spreading. The electronic identification and signature would remove the necessity of signing papers by hand.

The online courses arranged for Finnish officers are handy to make sure that every officer receives and learns the latest rules regulating the field. When reflecting this Finnish practice to the results of the CoE report published in 2013, it is evident that the Union legislation requires harmonization.

4.2.3 How the Finnish legislation is going to change due to the new Directive

In the beginning of 2017 it is still too early to evaluate how the new Directive will affect the Finnish national law. The Finnish Ministry of Justice has established a working group to form a proposal to the Finnish Government of the implementation of the new Directive to Finnish legislation.[400] The Senior Officer Mrs. Virpi Koivu, from the Police Department of the Ministry of the Interior, is currently participating in the organization formulating this proposal as the representative of the Police Department. According to Mrs. Koivu, at this point it is too early to say what is going to change in the current national legislation.[401]

Mr. Huhtiniemi, who is also participating to this working group with Mrs. Koivu, takes the same stand. But on a theoretical level Mr. Huhtiniemi thinks that the Finnish law is not likely to change much, if one looks only at the general principles.[402] The GDPR will replace the Finnish Personal Data Code (Henkilötietolaki 523/1999) at 25.5.2018 and presumably the Data Protection Directive on Police Matters will be implemented into the Finnish Act on the Processing of Personal Data by the Police (Laki henkilötietojen käsittelystä poliisitoimessa 761/2003).

[400] Oikeusministeriö, 12.1.2017.
[401] Koivu, 2017.
[402] Huhtiniemi, 2016.

Whether the protection of personal data and privacy are already at an adequate level in Finland from the perspective of police matters, Mr. Huhtiniemi cannot answer, because he doesn´t know what the terms "adequate" or "enough good" mean in this relation. He mentions that there is always something to fix, as some authorities leak information to the media and others utilize information without a work-related purpose.[403]

The Finnish law is already at the same level as required by the CJEU decisions *Digital Rights Ireland*[404] and *Tele2 Sverige AB*[405]. The Finnish authorities do not have legal grounds to gather personal data unless for specific purpose. President Niinistö referred in his speech to the current changes in the Finnish national legislation, especially to the forthcoming Data Collection Act which is currently being formulated but not yet in force, but the President also calls for the EU to act.[406] These CJEU's decisions will make it difficult for the Finnish legislator to write this new Act if it would allow general and indiscriminate collection of personal data. Mr. President´s request is confusing however, as on the one hand he is asking for more rights to gather personal data to protect national security and calling for the EU to act. At the same time the EU institutions are acting to ensure the high-level protection of Charter rights in the authorities' data processing and the CJEU is ordering the member states to remove their general data retention procedures.

4.3 Pros and cons of the uniform data protection legislation and the Directive

This chapter will introduce some points from the both sides of the uniform data protection legislation on police matters in the EU. Mr. Huhtiniemi states that time will tell as to how the implementation of the new Directive works out. He explains that the member states´ legislation on data protection in police matters differ from each other. The national authorities have different approaches to the aspects under the third pillar. As an example, some countries have stronger rules on secrecy and the data subjects do not have equally wide possibilities to access their personal data and some police sectors may be outside the supervision.[407]

[403] Ibidem.
[404] CJEU, Joined cases C-293/12 and C-594/12, Digital Rights Ireland, 8.4.2014.
[405] CJEU, Joined cases C-203/15 and C-698/15, Tele2 Sverige AB, 21.12.2016.
[406] New Year Speech by President of the Republic Sauli Niinistö, 1.1.2017.
[407] Huhtiniemi, 2016.

4.3.1 Possible problems in future

The EU member states still rely on mechanisms of cooperation based on norms that do not take into consideration the evolution of technologies. The police investigation will be complicated when it involves several jurisdictions as the legislation is not harmonized.[408] The Data Protection Directive on Police Matters states that it aims to uniform the level of protection of the natural persons´ rights in member states in relation to the processing of their personal data.[409] The EDPS stated that data protection in the police sectors should be consistent with the general rules written in the proposed GDPR[410] and be specified only if necessary. The Directive harmonizes at the minimum level. When member states can adopt legislation, which implements the Directive´s provisions differently than other states, it may create negative effects to the data subjects and unequal treatment between the member states.[411] Different standards of data protection will complicate the exchange of information and hinder the cooperation between the authorities. It is difficult to identify the individuals involved in the crime, the competent jurisdiction and to obtain evidence.

In the drafting process of the Data Protection Directive on Police Matters the EU Council included a sentence "*or the safeguarding against and the prevention of threats to public security*"[412] to the draft Directive, as a ground to interfere with individuals´ rights. This "*prevention of threats to public security*" can be interpreted to mean basically anything the current national public authority considers threatening, whether it is a threat or not. Nevertheless, this sentence was included in the final text. Mr. Huhtiniemi sees the "public security" and "national security" as evolving concepts. The legislators are not able to predict the development of the world in future, so their meanings should not be too strictly written in the law or it might narrow the authorities´ freedom of interpretation.[413]

The current trend in Europe is that the authorities want to gather more data.[414] Mr. Huhtiniemi states that the authorities already have access to a vast amount of data but the problem is that there are not enough resources to analyze even that. And the open internet

[408] Cocq, 2016, p. 185.
[409] EU Data Protection Directive on Police Matters 2016/680, Recital 7.
[410] EU Regulation 2016/679, General Data Protection Regulation.
[411] European Data Protection Supervisor Opinion 6/2015, 28.10.2015, p. 4-5.
[412] EU Council general approach 12555/15, 2.10.2015, p. 5.
[413] Huhtiniemi, 2016.
[414] Vainio, 2016, p. 251.

is only the tip of the iceberg. Under that there are the TOR and other secret and anonymous ways for the criminals to communicate online. The right answer is not to collect, for example everyone´s DNA into police files, but rather the measure has to be proportionate as the DNA of innocent people does not belong in the police files. Mr. Huhtiniemi asks what this would achieve and answers that the police could catch few suspects. It is not about confrontation but finding the right balance. When the authorities ask for more tools for gathering personal data, first the already existing tools should be evaluated, as to whether those are effective.[415]

But an innocent person should have nothing to hide. The problem with the "nothing to hide" argument is that it only considers the need to control personal facts. By compiling data from different sources, the authorities can form personal profiles about persons. These profiles may reveal sensitive facts and be used to predict future actions and to categorize someone as risk. Large-scale data collection presents risks because un-authorized persons can use that data. Different government data centers have been hacked and governments spy on each other. The problem is not the individual´s inability to hide facts from others but her inability to control how her data is used. The use of surveillance data is a problem of power imbalance.[416] As Lindroos-Hovinheimo says, privacy is like a gift that someone can give to the other.[417]

The fight against international terrorism to maintain international peace and security constitutes an objective of general interest, just as does the fight against serious crime to ensure public security. The fight against terrorism is important to ensure public security. Its effectiveness depends on the use of modern investigation techniques. But an objective of general interest does not justify a generalized data retention measure.[418] The states cannot adopt whatever measures they find appropriate, even to fight against terrorism. There has to exist adequate and effective guarantees against abuses.[419] At the time of 9/11 the threat of terrorism was serious. That is shown by both the wording of the UN resolutions of

[415] Huhtiniemi, 2016.
[416] Vainio, 2016, p. 252.
[417] Lindroos-Hovinheimo, 2016, p. 131.
[418] CJEU, Joined cases C-293/12 and C-594/12, Digital Rights Ireland, 8.4.2014, paras 42 & 51.
[419] ECtHR, No. 5029/71, Klass and Others v. Germany, 6.9.1978, para 42.

suspected terrorist organizations and the way they were adopted. However, the maintaining or reinforcement of those measures must be explained and justified convincingly.[420]

As Mr. Huhtiniemi points out, the new Directive allows wide possibilities to the member states to interpret the provisions. As an example, he points to the Directive´s Article 4[421], and its adjectives "specified" and "explicit" purposes as well as "adequate", "relevant", "not excessive" and "accurate". These are not clear and should not be written directly into the national law before first made concrete. Mr. Huhtiniemi asks what those adjectives mean and what the correct way to interpret them is. It is the CJEU´s task to assess, but everyone should be able to understand the final national legislation.[422]

Member states are able to adopt legislative measures to restrict the data subject´s access to her personal data, as long as such measures are justified, necessary and proportionate, and comply with the Charter and the ECHR, as interpreted in the case-law of the CJEU and the ECtHR.[423] Most of the EU member states have already transposed the main principles of the new Directive into their national law, thanks to the impact of the CoE Police Data Recommendation[424] and the Council Framework Decision 2008/977/JHA. So one can be skeptical as to whether the Directive is going to have real impact on legislation.[425] The future will show how they have implemented the Directive´s rules in their legislations and how the interpretations differ from each other.

4.3.2 Advantages of the uniform legislation

EU wide uniform legislation enables effective cooperation between the public authorities. Already in 2005, The Hague Programme fixed priorities for the Area of Freedom, Security and Justice, and described the principle of availability as the possibility for a member state´s public authority to obtain information from another member state.[426] The Commission commented in 2012 that the cross-border cooperation in police matters needs improvement. The legislation in the EU should be implemented Union wide and the Europol channel should be used systematically in the member states to create an EU-wide

[420] ECtHR, No. 10593/08, Nada v. Switzerland, 12.9.2012, para 186.
[421] EU Data Protection Directive on Police Matters 2016/680, Article 4. See footnote 323.
[422] Huhtiniemi, 2016.
[423] EU Data Protection Directive on Police Matters 2016/680, Recitals 40 & 43 - 46.
[424] CoE Police Data Recommendation Rec(87)15, 17.9.1987.
[425] Prof. Cannataci & Dr. Caruana, 2013, p. 52.
[426] The Hague Programme: 2005/C 53/01, OJ C 53, p. 1-14, 3.3.2005, Chapter 2.1.

picture of cross-border criminality.[427] When the products of the police investigation are in electronic form, that information can be shared among the authorities. This way it is possible to link different offences, offenders and incidents to each other. The advanced investigation is very much about finding patterns between incidents and crimes.

An anonymous source working in the international police cooperation presented the Spanish authorities as an example of a poor cooperation culture. The police departments around Spain do not exchange information effectively even between each other and the Catalonian authorities hardly communicate at all with the rest of Spain. As there are difficulties in national cooperation, it is natural that cooperation with foreign authorities is not any better. The purpose is not to shame Spain, but to clarify the general difficulties. The way personal data is collected, stored, and labeled, may influence the data subject´s presumption of innocence in case it is done in a careless manner. The new Directive orders the member states to establish the supervisory authorities. They should be able to bring these Directive´s infringements to the attention of the judicial authorities.[428] When these national authorities cooperate, it improves the security of individuals.

The CJEU strengthens the importance of a high level of protection of fundamental rights when data is processed in relation to national security and police matters.[429] Before the Data Protection Directive on Police Matters, this field was not uniformly regulated in the EU. The CoE member states, for example, do not have a common understanding of the term "*technical surveillance or other automated means*", and police practices vary between states as far as technical or other automated means of surveillance is concerned. Some CoE states have only some, or none, of their police systems available on-line.[430]

The new Directive eases the accomplishment of an area of freedom, security, and justice.[431] It harmonizes the member states legislations in the field. It sets the minimum level of regulation by stating in almost every Article, that the member states "shall provide" certain provisions in their domestic legislation. It aims to ensure that the natural

[427] EU Commission, Communication from the Commission to the European Parliament and the Council – Strengthening law enforcement cooperation in the EU: the European Information Exchange Model (EIXM), COM(2012) 735 final, 7.12.2012, Chapter 4.
[428] EU Data Protection Directive on Police Matters 2016/680, Recital 82-83.
[429] CJEU, Joined cases C-293/12 and C-594/12, Digital Rights Ireland, 8.4.2014, para 37, and CJEU, C-362/14, Schrems, 6.10.2015, para. 94.
[430] Prof. Cannataci & Dr. Caruana, 2013, p. 16 & 24.
[431] EU Data Protection Directive on Police Matters 2016/680, Recital 2.

persons´ level of protection of rights is equal in all member states in relation to the processing of their personal data.[432] The good side is that the member states must provide at least the same level of protection in their legislation. The new Directive and the GDPR supplement each other as they operate in different sectors but cooperate in the areas where they overlap. As an example, the Regulation applies when a competent authority lawfully discloses personal data to a recipient who is not a competent authority defined by the Directive.[433] Mr. Heikki Partanen states that the division of data protection law into the GDPR in commercial matters, and the Directive on police matters is a good idea. In police matters the aim is to identify unknown subject by processing her data, while in commercial matters the aim is to use the data to make individuals act in a certain manner, for example to buy the advertised good.[434]

The head of the EDPS Mr. Giovanni Buttarelli gave a supportive comment of the instrument in 2015. He stated that the rules in the Directive are consistent with the GDPR and the level of protection ensured by the Directive is at least at the same level as is currently ensured by other EU laws and instruments. Mr. Buttarelli explains that the EDPS wants the investigative authorities to be effective in the future and the smooth information sharing between the authorities is now more important than ever.[435] A multidisciplinary discussion is a priority because of the technical knowledge required in this field, a better cooperation with engineers and informatics is needed to maintain a human-rights-based approach. Policy makers, public authorities, companies, academics, technicians, programmers and individuals must cooperate to make the communication reliable.[436]

4.4 Conclusion of the section 4

The question of this thesis is whether the forthcoming Data Protection Directive on Police Matters ensures protection of the individual´s right to privacy. The answer is not yet clear. Mr. Huhtiniemi states that the adequacy of the protection must be viewed from the perspective of the whole Directive. Data protection law has to contain all the elements mentioned earlier in the previous pages. It has to contain the safeguards and legal remedies, the data subject´s access to the personal data and so on. It extends to the lifespan

[432] Ibid, Recital 7.
[433] Ibid, Recital 34.
[434] Partanen, 2016, p. 101-102.
[435] Buttarelli, Giovanni. European Data Protection Supervisor, 7.12.2015.
[436] Cocq, 2016, p. 198.

of the personal data and the whole chain of data processing has to be correct.[437] When information flows freely across national borders, the only way to protect those people whose information is being transmitted is to uniform the legislation between the member states. Smooth cooperation between law-enforcement authorities is important.

This section introduced the current national legislation dealing with data protection in the work of national public authorities by using the Finnish legislation as an example. The Finnish law already covers the data protection rules of the EU´s previous data protection instruments. The new Directive should not bring too many new changes in that sense, but the member states differ from each other with their legislation on this field. As the implementation process of the new Directive has only begun, it is too early to say what is going to change in the national legislations. As the Finnish system is at an adequate level already, it can be a good indication of where the other member states are heading towards. The new Directive will harmonize at the minimum level. The Finnish ministries have produced a pile of handbooks and manuals guiding the authorities´ work. It is likely that the other member states are about to face the same situation. Perhaps Finland can present the online course mentioned earlier as an effective tool to ensure that every national data processor and competent official knows the requirements of data protection. Secondly, the electronic investigation of crimes should rise in popularity among the authorities.

The national authorities may interfere with people´s fundamental rights if it is based on national security and public interest requirements. The fight against serious crime and terrorism is important to ensure public security and its effectiveness may depend on the use of modern investigation techniques. But an objective of general interest in itself does not justify an indiscriminate and generalized data retention measure.[438] It is for the national authorities and Courts to primarily interpret and apply the domestic law.[439] EU wide uniform legislation improves the cooperation between the authorities but the abstract Directive allows the member states to adopt legislations which differ from each other. This is likely to create negative effects and unequal treatment between the data subjects. Different standards hinder the cooperation between the authorities. When member states are forced to uniform their legislations and the instrument guiding the process is abstract, it is impossible to predict the outcome.

[437] Huhtiniemi, 2016.
[438] CJEU, Joined cases C-293/12 and C-594/12, Digital Rights Ireland, 8.4.2014, para 51.
[439] ECtHR, No. 11801/85, Kruslin v. France, 24.4.1990, paras 27 - 29.

THE CONCLUSION OF THE THESIS

The EU´s data protection law is under reform. The Union has adopted the GDPR to repeal the DPD, which is currently governing data protection in EU. The DPD applies to the processing of personal data in member states in the public and the private sectors, but it does not apply to activities in the areas of judicial and police cooperation in criminal matters. To fix this lack of scope the EU adopted the Data Protection Directive on Police Matters. It aims to ensure that the level of protection of individuals´ rights is equal in all member states in relation to the processing of their personal data in police matters.[440]

The question of this thesis is whether the new Directive ensures the protection of the right to privacy. The answer is three-folded. Firstly, it is too early to say as the new Directive is abstract and its implementation process is not ready. Secondly, it does, as the protection is already good in the Union´s legislative instruments and the new Directive only extends the data protection principles to cover the field of police matters. And thirdly, the implementation of the new Directive has problems because the member states´ national legislative systems and the cultures of application differ. Some countries, like Finland, have manuals and handbooks of data protection principles to be applied in practice and even compulsory courses which the officers must pass to be entitled to practice their profession. Some member states do not have such as was presented in the CoE report of the implementation of the CoE Police Data Recommendation.

The compressed list of the data protection principles, safeguards and findings

This thesis firstly introduced the current European legislation covering the investigative authorities work in relation to the protection of personal data and the protection of the right to privacy. It explained the operation of both relevant systems - the legislations of the CoE and the EU, and the main principles guiding the processing of personal data.

Secondly, this thesis went through the recent trends found in the European Courts in relation to the protection of personal data and privacy. It introduced the principles and interpretations established by the ECtHR and the CJEU, when national public authorities interfere with individual´s privacy in relation to data processing. Both Courts have similar

[440] EU Data Protection Directive on Police Matters 2016/680, Recital 7.

approach to the requirement of safeguards on measures interfering with individual´s rights. The national public authorities may interfere with an individual´s fundamental rights when fighting against serious crimes, but states cannot adopt whatever measures they find appropriate, even to fight against terrorism. The interference is justified if it is based on a national law provision which is precise, accessible to the concerned persons and its effects are foreseeable. The level of precision that is required of the law depends of the subject matter.[441] The legislation needs to govern the scope and application of measures interfering with individual´s privacy. The domestic legislation cannot provide for every eventuality, but it needs to have minimum safeguards against abuse concerning, inter alia, duration, storage, usage, third parties´ access, procedures for its destruction and for guarding the integrity and confidentiality of data. The data subject must be able to rely on that her data is accurate, processed in a lawful manner and disclosed only to authorized recipients. She must be able to fix possible faults in her data.

The fight against terrorism to maintain international peace and security constitutes an objective of general interest, just as does the fight against serious crime to ensure public security.[442] The Courts have been prudent with new technologies which enable wider possibilities for the authorities to interfere with individuals´ privacy. When personal data is processed by automated means the protection must be stronger. The fight against serious crime is important to ensure public security and its effectiveness may depend on the use of modern investigation techniques. The interference must refer to a pressing social need and be proportionate to the pursued legitimate aim. The national security interests may prevail over the individual ones, but an objective of general interest does not justify an indiscriminate and generalized data retention measure. Retained data must have at least some kind of a relationship to public security. The national legislation must be based on objective evidence of a certain public whose data is likely to reveal a link with serious crimes and to help in some way to fight these crimes or prevent a risk to public security.

Through those cases this thesis clarified the CJEU´s connection to the interpretations of the ECtHR. The CJEU has based its reasoning of the right to data protection and the right to respect of private life on the interpretations of the ECtHR. In the beginning the CJEU did not refer to the Charter but focused only on the ECHR. After 2009 when the Charter

[441] ECtHR, No. 6538/74, The Sunday Times v. UK, 26.4.1979, para 49, and ECtHR, No. 5947/72; 6205/73; 7052/75; 7061/75; 7107/75; 7113/75, Silver and Others v. UK, 25.3.1983, para 88.
[442] CJEU, Joined cases C-293/12 and C-594/12, Digital Rights Ireland, 8.4.2014, para 42.

acquired the status of primary EU law, the CJEU began to move away from the ECHR and to use it as the main instrument to interpret the rights to data protection and privacy.

Thirdly, this thesis introduced how the EU´s legislation on data protection is changing. Specifically, it focused on introducing the forthcoming Data Protection Directive on Police Matters. And then fourthly, the thesis collected information to protect the core claim of the thesis, that the forthcoming Directive does protect the right to privacy.

The concept of the adequate protection of privacy

Inspector general Huhtiniemi, from the Office of the Finnish Data Protection Ombudsman, says that the adequate protection of privacy does not yet have a definition. It is the CJEU´s task to assess. Mr. Huhtiniemi looks at the adequacy of the protection of privacy from the perspective of the whole instrument - in this case the new Directive. The protection is not established in one specific Article. The data protection law must contain all the elements and safeguards mentioned earlier. The protection of privacy in practice comes from all the aspects gone through in this thesis and it extends to the lifespan of the personal data. The evaluation is conducted on a case-by-case basis and the whole chain of data processing must be right. The level of protection of privacy must be evaluated in practice.

The DPD supports this view in relation to transmitting personal data from EU to a third country. When personal data is sent from EU member states to a third country, that transfer may take place only if the receiving state ensures a level of protection of privacy that is adequate, i.e. essentially equivalent to that guaranteed within the EU. The DPD Article 25(2) states that the adequacy of the protection shall be assessed "*in the light of all the circumstances surrounding a data transfer*". The national law must provide adequate protection against arbitrary interference of privacy. "*This assessment depends on all the circumstances of the case, such as the nature, scope and duration of the possible measures, the grounds required for ordering them, the authorities competent to permit, carry out and supervise them, and the kind of remedy provided by the national law*".[443]

The head of the EDPS Mr. Buttarelli has stated that the rules in the new Directive are consistent with the GDPR and the level of protection ensured by the Directive is at least at

[443] ECtHR, No. 35623/05, Uzun v. Germany, 2.9.2010, paras 60-63.

the same level as is currently ensured by other EU laws and instruments. The assurance that the protection of privacy will be at least at the same level in the future indicates that the current level of protection is good.

The implementation of the new Directive is still far and out of reach

The member states may face problems when implementing the new Directive into their national legislations. As Mr. Huhtiniemi points out, the Directive allows wide possibilities to the member states to interpret the provisions. The terms in the instrument are not clear and should not be written directly into the national legislation but first made concrete. When member states can adopt legislation, which implements the Directive´s provisions differently than other states, it may create negative effects to the data subjects and unequal treatment between the states. Different levels of data protection standards will complicate the exchange of information and hinder the cooperation between the authorities.

The new Directive does not harmonize the field as much as the GDPR would do if the GDPR also contained the field covered by the Directive. The protection of privacy would be unacceptably weakened if the use of modern techniques in the criminal-justice system were allowed without balancing the possible benefits of the extensive use of such techniques against privacy interests. A state which claims to be a pioneer in the development of new technology should find the right balance in this regard.[444] The Finnish obligatory online course is good way to ensure that every officer dealing with personal data does know what she can do to it and with it.

At this point it is too early to fully answer whether the new Directive ensures adequate protection to privacy as it is not yet in force. When member states are forced to uniform their legislation, which are characterized by their own legislative and cultural traditions, and the instrument guiding the process is abstract, it is impossible to predict the outcome. A good intention may result in bad consequences. The national organs interpret the provisions of the new Directive and then after the Directive is in force someone might raise a question to the CJEU and ask if it was implemented correctly in the national laws. The future will show how the member states implemented the Directive´s rules and how the interpretations differ from each other. Further research is needed to find the answers.

[444] ECtHR, No. 30562/04 and 30566/04, S. and Marper v. UK, 4.12.2008, paras 111-112.

LIST OF REFERENCES

Arai-Takahashi, Y. The Margin of Appreciation Doctrine and the Principle of Proportionality in the Jurisprudence of the ECHR. Intersentia. 2001.

Article 29 Working Party Opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT), WP 128. 22.11.2006.

Article 29 Working Party Opinion 1/2010 on the concepts of 'controller' and 'processor', WP 169. 16.2.2010.

Article 29 Working Party Opinion 3/2010 on the principle of accountability, WP 173. 13.7.2010.

Article 29 Working Party Opinion 15/2011 on the notion of consent, WP 187. 13.7.2011.

Article 29 Working Party Opinion 03/2013 on purpose limitation, WP 203. 2.4.2013.

Barnard, C. The Substantive law of the EU, The four freedoms. 4th edition. Oxford. 2013

Benyekhlef, K. Les normes internationales de protection des données personnelles et l'autoroute de l'information. Les Journées Maximilien-Caron: Le respect de la vie privée dans l'entreprise, 65–101. Thémis. 1996.

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. Helsinki: Helsingin yliopiston oikeustieteellisen tiedekunnan julkaisut. 2016.

Buttarelli, G. European Data Protection Supervisor. Video: EU Data Protection Reform: The Directive on police, justice and criminal matters. Youtube. 7.12.2015. Online: https://www.youtube.com/watch?v=_Q19JtF3ieI&feature=youtu.be, 27.11.2016.

Charter of fundamental rights of the European Union, 2012/C 326/02, 2009. OJ C 326, p. 391–407, 26.10.2012.

CJEU, C-101/01, Bodil Lindqvist, ECLI:EU:C:2003:596. 6.11.2003.

CJEU, C-275/06, Productores de Música de España (Promusicae) v. Telefónica de España SAU. 29.1.2008.

CJEU, C 73/07, Opinion of advocate General Kokott, on case Tietosuojavaltuutettu v. Satakunnan Markkinapörssi Oy and Satamedia Oy, ECLI:EU:C:2008:266. 8.5.2008.

CJEU, C-73/07, Tietosuojavaltuutettu v. Satakunnan Markkinapörssi Oy and Satamedia Oy, ECLI:EU:C:2008:727. 16.12.2008.

CJEU, C-553/07, College van burgemeester en wethouders van Rotterdam v. M. E. E. Rijkeboer, ECLI:EU:C:2009:293. 7.5.2009.

CJEU, C-553/07, Opinion of Advocate General Ruiz-Jarabo Colomer, in case College van burgemeester en wethouders van Rotterdam v. M.E.E. Rijkeboer, ECLI:EU:C:2008:773. 22.12.2008.

CJEU, Joined Cases C-92/09 and C 93/09, Opinion of Advocate General Sharpston on Schecke and Eifert, ECLI:EU:C:2010:353. 17.6.2010.

CJEU, Joined cases C-92/09 and C-93/09, Volker and Markus Schecke GbR and Hartmut Eifert v. Land Hessen, (Schecke and Eifert) ECLI:EU:C:2010:662. 9.11.2010.

CJEU, C-543/09, Deutsche Telekom AG v. Germany, ECR I-3441. 5.5.2011.

CJEU, C-70/10, Opinion of Advocate General Cruz Villalón in Case Scarlet, ECLI:EU:C:2011:255. 14.4.2011.

CJEU, C-70/10, Scarlet Extended SA v. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM), (Scarlet) ECLI:EU:C:2011:771. 24.11.2011.

CJEU, Joined cases C-468/10 and C-469/10, Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) & Federación de Comercio Electrónico y Marketing Directo (FECEMD) v. Administración del Estado. 24.11.2011.

CJEU, C-614/10 Commission v. Austria, ECLI:EU:C:2012:631. 16.10.2012.

CJEU, Joined cases C-293/12 and C-594/12, Digital Rights Ireland and Seitlinger, ECLI:EU:C:2014:238. 8.4.2014.

CJEU, C-362/14, Opinion of Advocate General, Maximillian Schrems v. Data Protection Commissioner, ECLI:EU:C:2015:627. 25.9.2015.

CJEU, C-362/14, Maximillian Schrems v. Data Protection Commissioner (Schrems), ECLI:EU:C:2015:650. 6.10.2015.

CJEU, Joined cases C-203/15 and C-698/15, Tele2 Sverige AB, ECLI:EU:C:2016:970. 21.12.2016.

Cocq, C. C. Encryption and anonymisation online: challenges for law enforcement authorities within the EU. T. Bräutigam & S. Miettinen, Data Protection, Privacy and European Regulation in the Digital Age, p. 178-204. Helsinki: Helsingin yliopiston oikeustieteellisen tiedekunnan julkaisut. 2016.

CoE Convention on Cybercrime CETS No. 185, Committee of Ministers, entered into force on 1.7.2004. 23.11.2001.

CoE Recommendation Rec (87)15 to member states regulating the use of personal data in the police sector, Committee of Ministers. 17.9.1987.

Convention 108, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Council of Europe, CETS No. 108. 1981.

Council of Europe, Treaty office. Full list, Chart of signatures and ratifications of Treaty 108, Status as of 3.9.2016. www.coe.int. 2016. Online: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures?p_auth=JaBAQTad, 3.9.2016.

EC Treaty, Treaty establishing the European Community, 2002. OJ C 325, 24.12.2002, p. 33–184.

ECHR Protocol No. 11 to the Convention for the Protection of Human Rights and Fundamental Freedoms, restructuring the control machinery established thereby, ETS No.155. 1.11.1998.

ECHR Reform, Margin of Appreciation, An overview of the Strasbourg Court's margin of appreciation doctrine. www.justiceinitiative.org . 2012. Online: https://www.opensocietyfoundations.org/sites/default/files/echr-reform-margin-of-appreciation.pdf, 10.9.2016.

ECHR, European Convention on Human Rights. Council of Europe. 1950.

ECtHR, No. 5029/71, Klass and Others v. Germany. 6.9.1978.

ECtHR, No. 5493/72, Handyside v. UK. 7.12.1976.

ECtHR, No. 5947/72; 6205/73; 7052/75; 7061/75; 7107/75; 7113/75, Silver and Others v. UK. 25.3.1983.

ECtHR, No. 6538/74, The Sunday Times v. UK. 26.4.1979.

ECtHR, No. 7525/76, Dudgeon v. UK. 22.10.1981.

ECtHR, No. 8691/79, Malone v. UK. 2.8.1984.

ECtHR, No. 9248/81, Leander v. Sweden. 26.3.1987.

ECtHR, No. 10737/84, Müller and Others v. Switzerland. 24.5.1988.

ECtHR, No. 11801/85, Kruslin v. France. 24.4.1990.

ECtHR, No. 23224/94, Kopp v. Switzerland. 25.3.1998.

ECtHR, No. 27798/95, Amann v. Switzerland. 16.2.2000.

ECtHR, No. 28341/95, Rotaru v. Romania. 4.5.2000.

ECtHR, No. 44647/98, Peck v. UK. 28.1.2003.

ECtHR, No. 44787/98, P.G. and J.H. v. UK. 25.9.2001.

ECtHR, No. 50774/99, Sciacca v. Italy. 11.1.2005.

ECtHR, No. 59320/00, Von Hannover v. Germany. 24.6.2004.

ECtHR, No. 71611/01, Wisse v. France. 20.12.2005.

ECtHR, No. 2346/02, Pretty v. UK. 29.4.2002.

ECtHR, No. 2872/02, K.U. v. Finland. 2.12.2008.

ECtHR, No. 25198/02, Iordachi and Others v. Moldova. 10.2.2009.

ECtHR, No. 20511/03, I. v. Finland. 17.7.2008.

ECtHR, No. 21737/03, Haralambie v. Romania. 27.10.2009.

ECtHR, No. 30562/04 and 30566/04, S. and Marper v. UK. 4.12.2008.

ECtHR, No. 32881/04, K.H. and Others v. Slovakia. 28.4.2009.

ECtHR, No. 6339/05, Evans v. UK. 7.3.2006.

ECtHR, No. 35623/05, Uzun v. Germany. 2.9.2010.

ECtHR, No. 420/07, Köpke v. Germany. 5.10.2010.

ECtHR, No. 10593/08, Nada v. Switzerland. 12.9.2012.

ECtHR, No. 36769/08, Ashby Donald and others v. France. 10.1.2013.

ECtHR, No. 39954/08, Axel Springer AG v. Germany [GC]. 7.2.2012.

ECtHR, No. 40660/08 and 60641/08, Von Hannover v. Germany (No. 2) [GC]. 7.2.2012.

EU Commission Action Plan Implementing the Stockholm Programme, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. COM 171 final. 20.4.2010.

EU Commission Communication from the Commission to the European Parliament and the Council on the follow-up of the Work Programme for better implementation of the Data Protection Directive. COM 87 Final. 7.3.2007.

EU Commission Communication from the Commission to the European Parliament and the Council—Area of Freedom, Security and Justice serving the citizen. COM 262 Final. 10.6.2009.

EU Commission Communication from the Commission: Strategy for the effective implementation of the Charter of Fundamental Rights by the European Union. COM 573. 19.10.2010.

EU Commission Communication to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions: A comprehensive approach on personal Data Protection in the European Union. COM 609 final. 4.11.2010.

EU Commission Communication: Safeguarding privacy in a connected world: A European Data Protection framework for the 21st Century. COM 9 final. 25.1.2012.

EU Commission Communication from the Commission to the European Parliament and the Council – Strengthening law enforcement cooperation in the EU: the European Information Exchange Model (EIXM), COM 735 final. 7.12.2012.

EU Commission Decision, 2000/520/EC, of 26.7.2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce (notified under document number C(2000) 2441) (Text with EEA relevance.) OJ L 215, 25.8.2000 P. 7 – 47.

EU Commission First report on the implementation of the Data Protection Directive 95/46/EC. COM 265 final. 15.5.2003.

EU Commission Impact Assessment, SEC (2012) 72 final. Accompanying the document: Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) and Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data. 25.1.2012.

EU Commission Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data Proposal for a General Data Protection Regulation (Data Protection Directive on Police Matters). COM 10 final, 25.1.2012.

EU Commission Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). COM 11 final. 25.1.2012.

EU Council Act 2000/C 197/01, establishing in accordance with Article 34 of the Treaty on European Union the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union, 29.5.2000. OJ C 197, 12.7.2000, p. 1.

EU Council Decision 2000/642/JHA, of 17.10.2000 concerning arrangements for cooperation between financial intelligence units of the Member States in respect of exchanging information. OJ 2000 L 271, 24.10.2000, p. 4-6.

EU Council Decision 2002/187/JHA, of 28.2.2002 setting up Eurojust with a view to reinforcing the fight against serious crime. OJ 2002 L 63, 6.3.2002, p. 1-13.

EU Council Decision 2003/659/JHA, of 18.6.2003 amending Decision 2002/187/JHA setting up Eurojust with a view to reinforcing the fight against serious crime. OJ L 245, 29.9.2003, p. 44.

EU Council Decision 2007/533/JHA, SIS-II, of 12.6.2007 on the establishment, operation and use of the second generation Schengen Information System, OJ 2007 L 205. 7.8.2007, p. 63-84.

EU Council Decision 2008/615/JHA; Prüm Decision, of 23.6.2008 on the stepping up of cross-border cooperation, particularly in combating terrorism and cross-border crime. OJ L 210, 6.8.2008, p. 1-11.

EU Council Decision 2009/371/JHA, of 6.4.2009 establishing the European Police Office (Europol). OJ L 121. 15.5.2009, p. 37-66.

EU Council Decision 2009/426/JHA, of 16.12.2008 on the strengthening of Eurojust and amending Decision 2002/187/JHA setting up Eurojust with a view to reinforcing the fight against serious crime. OJ 2009 L 138. 4.6.2009, p. 14-32.

EU Council Decision 2009/917/JHA, CIS Decision, of 30.11.2009 on the use of information technology for customs purposes. OJ 2009 L 323, 10.12.2009, p. 20-30.

EU Council Framework Decision 2008/977/JHA, of 27.11.2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters. OJ 2008 L 350, 30.12.2008, p. 60–71.

EU Council Framework Decision 2009/315/JHA, of 26.2.2009 on the organisation and content of the exchange of information extracted from the criminal record between Member States. OJ 2009 L 93, 7.4.2009, p. 23-32.

EU Council general approach 12555/15. Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties and the free movement of such data, 2012/0010 (COD). 2.10.2015.

EU Declaration No 1 concerning the Charter of Fundamental Rights of the European Union, annexed to the Final Act of the Intergovernmental Conference which adopted the Treaty of Lisbon. 13.12.2007.

EU Declaration No 21 concerning the Charter of Fundamental Rights of the European Union, annexed to the Final Act of the Intergovernmental Conference which adopted the Treaty of Lisbon. 13.12.2007.

EU Directive 95/46/EC, (Data Protection Directive) of the European Parliament and of the Council of 24.10.1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. OJ L 281, 23.11.1995, p. 31 - 50.

EU Directive 2002/22/EC, (Universal Service Directive) of the European Parliament and of the Council of 7.3.2002 on universal service and users' rights relating to electronic communications networks and services. OJ L 108, 24.4.2002, p. 51–77.

EU Directive 2002/58/EC, (Directive on privacy and electronic communications) of the European Parliament and of the Council of 12.7.2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector. OJ L 201, 31.7.2002, p. 37 - 47.

EU Directive 2006/24/EC, (Data Retention Directive) of the European Parliament and of the Council of 15.3.2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC. OJ 2006 L105, 13.4.2006, p. 54-63.

EU Directive 2009/136/EC, of the European Parliament and of the Council of 25.11.2009 amending Directive 2002/22/EC on universal service and users’ rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities

responsible for the enforcement of consumer protection laws. OJ 2009 L 337, 18.12.2009, p. 11-36.

EU Directive 2016/680, (Data Protection Directive on Police Matters) of the European Parliament and of the Council of 27.4.2016 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. OJ L 119, 4.5.2016, p. 89–131.

EU Parliament Debates. 13. Protection of individuals with regard to the processing of personal data - Processing of personal data for the purposes of crime prevention (debate). 11.3.2014. Online: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+CRE+20140311+ITEMS+DOC+XML+V0//EN&language=EN, 8.2.2017.

EU Parliament, Resolution on the Communication from the Commission to the European Parliament and the Council – An area of freedom, security and justice serving the citizen – Stockholm programme. 25.11.2009.

EU Regulation (EC) 2725/2000 of 11.12.2000 concerning the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of the Dublin Convention. OJ L 316, 15.12.2000, p. 1 - 10.

EU Regulation (EC) 45/2001 of the European Parliament and of the Council of 18.12.2000 on the protection of individuals with regard to the processing of personal data by the institutions and bodies of the Community and on the free movement of such data. OJ L 8, 12.1.2001, p. 1.

EU Regulation (EC) 407/2002 of 28.2.2002 laying down certain rules to implement Regulation (EC) 2725/2000 concerning the establishment of "Eurodac" for the comparison of fingerprints for the effective application of the Dublin Convention. OJ L 62, 5.3.2002, p. 1–5.

EU Regulation (EC) 767/2008, (VIS Regulation) of the European Parliament and of the Council of 9.7.2008 concerning the Visa Information System (VIS) and the exchange of data between Member States on short-stay visas. OJ L 218/60, 13.8.2008, p. 1-22.

EU Regulation 1052/2013 of the European Parliament and of the Council of 22.10.2013 establishing the European Border Surveillance System (Eurosur). OJ L 295, 6.11.2013, p. 11–26.

EU Regulation 2016/679, (General Data Protection Regulation) 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 and on the free movement of such data, and repealing Directive 95/46/EC. OJ L 119, 4.5.2016, p. 1-88.

European Data Protection Supervisor (EDPS), Overview. European Union, online: https://europa.eu/european-union/about-eu/institutions-bodies/european-data-protection-supervisor_en. 20.8.2016.

European Data Protection Supervisor Opinion 6/2015. A further step towards comprehensive EU data protection, recommendations on the Directive for data protection in the police and justice sectors, 28.10.2015.

European Union Agency for Fundamental Rights and Council of Europe, Handbook on European data protection law. Luxembourg. 2014.

Explanations Relating to the Charter of Fundamental Rights. OJ 2007 C 303, 14.12.2007, p. 17-35.

Franssen, V. The future of national data retention obligations – How to apply Digital Rights Ireland at national level? The European Law Blog, 25.7.2016. Online: http://europeanlawblog.eu/2016/07/25/the-future-of-national-data-retention-obligations-how-to-apply-digital-rights-ireland-at-national-level/, 11.1.2017.

Full list, Chart of signatures and ratifications of Treaty 185, Convention on Cybercrime, Council of Europe. 2.10.2016. Online: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures, 2.10.2016.

Fuster, G. G. The Emergence of Personal Data Protection as a Fundamental Right of the EU. Switzerland: Springer International Publishing. 2014.

Gilbert, F. Privacy v. Data Protection. What is the Difference? Francoise Gilbert on privacy, security and cloud computing, 1.10.2014. Online: http://www.francoisegilbert.com/2014/10/privacy-v-data-protection-what-is-the-difference/, 3.9.2016.

Henkilötietolaki 523/1999.

Huhtiniemi, H. Interview, 29.12.2016. Topic: Level of data protection in Finland and in EU. Interviewer: Pajunoja, L.

Koivu, V. Interview, 25.1.2017. Topic: Representative of the Police Department of the Ministry of the Interior in the working group formulating the proposal of the national legislation based on the Data Protection Directive on Police Matters. Interviewer: Pajunoja, L.

Laki henkilötietojen käsittelystä poliisitoimessa 761/2003.

Laki poliisin henkilörekistereistä 509/1995.

Laki viranomaisten toiminnan julkisuudesta 621/1999.

Laraine, L. Summaries of EU court decisions relating to data protection 2000-2015. OLAF Data Protection Officer, 2016. Online: https://ec.europa.eu/anti-fraud/sites/antifraud/files/caselaw_2001_2015_en.pdf, 30.10.2016.

Lindroos-Hovinheimo, S. Elämäntarinoiden hallintaa - Eurooppalainen henkilötietojen suoja yksilöllistymisen ilmentäjänä. Viestintäoikeuden vuosikirja 2015. (U. Oy, Toim.) Helsinki: Helsingin yliopiston oikeustieteellinen tiedekunta. 2016.

Lynskey, O. Joined Cases C-293/12 and 594/12 Digital Rights Ireland and Seitlinger and Others: The Good, the Bad and the Ugly. European Law Blog, 8.4.2014. Online: http://europeanlawblog.eu/2014/04/08/joined-cases-c-29312-and-59412-digital-rights-ireland-and-seitlinger-and-others-the-good-the-bad-and-the-ugly/, 11.1.2017.

Määräys poliisin salassa pidettävien tietoaineistojen käsittely POL-2015-3101. Poliisihallitus. 3.6.2015.

Määräys poliisin tietojärjestelmien käyttö ja ylläpito 2020/2012/1302. Poliisihallitus. 13.2.2013.

Määräys rekisterinpito poliisissa 2020/2011/1423. Poliisihallitus. 26.5.2011.

Määräys sähköpostin käyttöperiaatteet sisäasianministeriön hallinnonalalla SMDno/2012/806. Sisäasianministeriö. 11.2.2013.

Määräys tietoturvahäiriöiden hallinta poliisissa 2020/2012/1303. Poliisihallitus. 13.2.2012.

Neacşu, D. European Human Rights System. Arthur W. Diamond Law Library Research Guides, 4.2.2015. Online: http://library.law.columbia.edu/guides/European_Human_Rights_System#In_Print_at_Columbia_4, 11.9.2016.

New Year Speech by President of the Republic Sauli Niinistö. 1.1.2017.

Nissenbaum, H. Protecting Privacy in an Information Age: The Problem of Privacy in Public. Law and Philosophy, 17: 559-596. Princeton University. 1998.

OECD Guidelines on governing the Protection of Privacy and transborder flows of personal data, C(80)58/FINAL, as amended on 11.7.2013 by C(2013)79. 2013.

Ohje poliisin tietojen käytöstä virkatehtävissä, POL-2016-4458. Poliisihallitus. 18.04.2016.

Ohje rekisteröidyn oikeuksien toteuttaminen poliisissa: tarkastusoikeus, tiedon korjaaminen ja informointi 2020/2012/66. Poliisihallitus. 23.1.2012.

Ohje tietojen kirjaaminen poliisiasiain tietojärjestelmään (PATJA) 2020/2013/5231. Poliisihallitus. 17.12.2013.

Oikeusministeriö. EU:n tietosuojadirektiivin täytäntöönpano, OM 21/41/2016. 12.1.2017.

Oikeusministeriö. Poliisi- ja oikeusviranomaisten käsittelemien, rikosasioihin liittyvien henkilötietojen suojaaminen. 12.10.2016. Online: http://www.oikeusministerio.fi/fi/index/valmisteilla/lakihankkeet/informaatio-oikeus/tietosuojapuitepaatos.html, 17.11.2016.

Partanen, H. Henkilötietojen kategoriat ja käsittelyn suunnat - Henkilötieto-oikeuden tieto-opillisia kysymyksiä. Viestintäoikeuden vuosikirja 2015. (Unigrafia, Ed.) Helsinki: Oikeustieteellinen tiedekunta. 2016.

Perustuslaki 731/1999.

Poliisiammattikorkeakoulu. Poliisi (AMK) -tutkinto opetussuunnitelma lukuvuosi 2016–2017. Poliisiammattikorkeakoulu. 2016.

Poliisihallitus. Poliisin tietoturvapolitiikka (2020/2010/4157). 2010.

Poliisilaki 872/2011.

Prof. Cannataci, J. A. & Dr. Caruana, M. M. Report: Recommendation R (87) 15 – Twenty–five years down the line. Council of Europe. 2013.

Reinboth, S. Poliisit urkkivat Mika Myllylän tietoja uteliaisuuttaan. Helsingin Sanomat, 27.3.2014. Online: http://www.hs.fi/kotimaa/a1395890187170, 16.8.2016.

Rikoslaki 39/1889.

Rosas, A. & Armati, L. EU Constitutional Law, An introduction. 2nd edition. Oxford. 2012.

Sajari, P. EU:n tuomioistuin: Valtiot loukanneet yksityisyyden suojaa internetissä – ratkaisulla vaikutuksia myös Suomeen. Helsingin Sanomat, 21.12.2016. Online: http://www.hs.fi/ulkomaat/art-2000005016509.html, 13.1.2017.

Summary of Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. CoE Treaty office, 28.1.1981. Online: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108, 20.8.2016.

TEU, Treaty on the European Union. 2012. OJ C 326, 26.10.2012, p. 1-39.

TFEU, Treaty on the Functioning of the European Union. 2012. OJ C326, 26.10.2012, p. 47–390.

The Council of Europe in brief, Who we are. Council of Europe, 2016. Online: http://www.coe.int/en/web/about-us/who-we-are, 3.9.2016.

The Hague Programme: strengthening freedom, security and justice in the European Union. 2005/C 53/01. OJ C 53, 3.3.2005, p. 1-14.

The Stockholm Programme: an open and secure Europe serving and protecting citizens. 2010/C 115/01. OJ C 115, 4.5.2010, p. 1-38.

Treaty of Lisbon amending the TEU and the Treaty establishing the European Community, 13.12.2007. OJ C 306, 17.12.2007, p. 1–271.

UNHCR, Council of Europe: European Commission on Human Rights. www.refworld.org, 2016. Online: http://www.refworld.org/publisher/COECOMMHR.html, 11.9.2016.

Vainio, N. Fundamental rights compliance and the politics of interpretation: Explaining Member State and court reactions to Digital Rights Ireland. T. Bräutigam & S. Miettinen, Data Protection, Privacy and European Regulation in the Digital Age, p. 229-260. Helsinki: Helsingin yliopiston oikeustieteellisen tiedekunnan julkaisut. 2016.

What is an EU Directive? Europeanlawmonitor.org. Online: http://www.europeanlawmonitor.org/what-is-guide-to-key-eu-terms/eu-legislation-what-is-an-eu-directive.html, 28.8.2016.