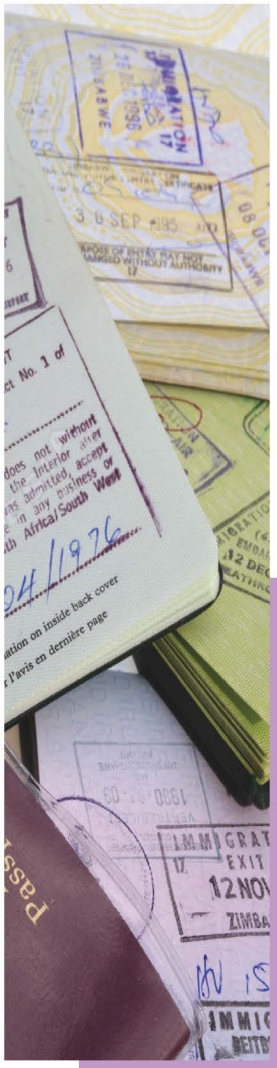
European Parliament

DIRECTORATE-GENERAL FOR INTERNAL POLICIES

POLICY DEPARTMENT C
CITIZENS' RIGHTS AND CONSTITUTIONAL AFFAIRS



Constitutional Affairs

Justice, Freedom and Security

Gender Equality

Legal and Parliamentary Affairs

Petitions

A Comparison between US and EU Data Protection Legislation for Law Enforcement

Study for the LIBE Committee

EN

2015

DIRECTORATE GENERAL FOR INTERNAL POLICIES

POLICY DEPARTMENT C: CITIZENS' RIGHTS AND CONSTITUTIONAL AFFAIRS

CIVIL LIBERTIES, JUSTICE AND HOME AFFAIRS

A comparison between US and EU data protection legislation for law enforcement purposes

STUDY

Abstract

This study was commissioned by the European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs at the request of the LIBE Committee. The study compares US and the EU legal frameworks on data protection in the field of law enforcement. It reviews US and EU principal legal sources of data protection legislation in the law enforcement and national security context and identifies rights available to individuals. The study further considers newly introduced or proposed US laws such as the USA FREEDOM Act and the Draft Judicial Redress Act and reviews its compatibility with EU data protection standards.

DOCUMENT REQUESTED BY THE
COMMITTEE ON CIVIL LIBERTIES, JUSTICE AND HOME AFFAIRS (LIBE)

AUTHORS

Prof. Dr. Franziska Boehm, University of Münster, Institute for Information, Telecommunication and Media Law, Germany

With the help of Markus Andrees, Jakob Beaucamp, Tim Hey, Robert Ortner, Giulia Priora and Felix Suwelack.

RESPONSIBLE ADMINISTRATOR

Mr Alessandro DAVOLI
Policy Department C - Citizens' Rights and Constitutional Affairs
European Parliament
B-1047 Brussels
E-mail: poldep-citizens@europarl.europa.eu

LINGUISTIC VERSIONS

Original: EN

ABOUT THE EDITOR

Policy Departments provide in-house and external expertise to support EP committees and other parliamentary bodies in shaping legislation and exercising democratic scrutiny.

To contact the Policy Department or to subscribe to its monthly newsletter please write to:
poldep-citizens@europarl.europa.eu

European Parliament, manuscript completed in September 2015.

This document is available on the Internet at:
http://www.europarl.europa.eu/studies

DISCLAIMER

CONTENTS

LIST OF ABBREVIATIONS

ADR	Alternative Dispute Resolution
CFR	Charter of Fundamental Rights of the European Union
CIA	Central Intelligence Agency
CJEU	Court of Justice of the European Union
Commission	European Commmision
DDPLE	Proposed Directive for Data Protection in Law Enforcement
DRD	Data Retention Directive
ECHR	European Convention on Human Rights
ECPA	Electronic Communications Privacy Act
ECtHR	European Court of Human Rights
EDPB	European Data Protection Board
EDPS	European Data Protection Supervisor
EP	European Parliament
FBI	Federal Bureau of Investigation
FISA	Foreign Intelligence Surveillance Act
FTC	Federal Trade Commission
GDPR	Proposed General Data Protection Regulation
LE	Law enforcement
NSL	National Security Letter
PNR	Passenger Name Record
PPD	Presidential Policy Directive
SIS	Schengen Information System
SH	Safe Harbor

SWIFT	Society for Worldwide Interbank Financial Telecommunications
TFEU	Treaty on the Functioning of the European Union
TFTP	Terrorist Finance Tracking Program

EXECUTIVE SUMMARY

This study compares EU and US data protection guarantees in the field of law enforcement. The legal approaches to regulate data protection guarantees in law enforcement, in both the EU and the US legal order, vary from their very outset, leading to structural, legal and in particular constitutional differences.

Generally, it can be concluded that the EU data protection framework in the law enforcement sector is shaped by comprehensive data protection guarantees, which are codified in EU primary and secondary law and are accompanied by EU and ECtHR case law. In contrast, US data protection guarantees in the law enforcement and national security contexts are sector specific and are therefore contained within the specific instruments which empower US agencies to process personal data. They vary according to the instruments in place and are far less comprehensive.

Above all, constitutional protection is limited. US citizens may invoke protection through the Fourth Amendment and the Privacy Act, but the data protection rights granted in the law enforcement sector are limitedly interpreted with a general tendency to privilege law enforcement and national security interests. Moreover, restrictions to data protection in the law enforcement sector are typically not restricted by proportionality considerations, reinforcing the structural and regular preference of law enforcement and national security interests over the interests of individuals. Regarding the scope and applicability of rights, non-US persons are usually not protected by the existing, already narrowly interpreted, guarantees. The same is true with regards to other US law. When data protection guarantees do exist in federal law, they usually do not include protection for non-US persons.

A majority of the EU data protection standards cannot be found in US law. For instance, rules limiting inter-agency data exchange, exchanges with other third parties, completely independent oversight, strict proportionality rules and effective judicial review possibilities and information requirements for non-US persons on surveillance or data breaches or effective access, and correction and deletion rights simply do not exist at all or are, at best, very limited. These shortcomings are also visible regarding existing data exchange agreements between the US and the EU, such as, for instance, the Safe Harbor regime. Its principles do not necessarily comply with the current EU data protection standards.

In particular, the approach to data sharing is fundamentally different. Whereas in EU law every transfer of data to other agencies interferes with fundamental rights and requires specific justification, data sharing in the US between law enforcement authorities and the intelligence community seems to be the rule rather than the exception.

Recently introduced US laws such as the Draft Judicial Redress Act or the FREEDOM Act do not fundamentally alter these findings. Whilst the Draft Judicial Redress Act is limited in scope and requires some clarification, the FREEDOM Act is mainly designed to improve the protection of US citizens in the framework of intelligence collection activities. Furthermore, only three out of the four remedies of the Privacy Act are available to EU individuals in the framework of the Draft Judicial Review Act, leaving an individual with no judicial review possibilities in case an agency fails to provide an accurate, relevant, timely and complete treatment of the individual's data.

Nonetheless, the introduction of stricter access requirements in the FREEDOM Act using a specific selection term for the collection of tangible things and metadata for foreign intelligence purposes is an improvement compared to the former provisions. Regrettably,

this newly introduced restriction does not affect Section 702 of the FISA Amendment Act or Executive Order 12333, which still authorize far-reaching surveillance of foreign intelligence information, including the accessing of communications, content, metadata or other records by governmental agencies. A future instrument regulating EU-US data exchange should address the mentioned issues, as serious concerns about their compatibility with EU fundamental rights arise.

It can be also deduced, from the comparison, that even if all existing US data protection guarantees in the law enforcement and national security framework were applicable to EU citizens, there would still remain a considerable shortcoming regarding the level of privacy and personal data protection compared to the protection through EU law. Recent proposals and changes through the Draft Judicial Redress Act of 2015 and the FREEDOM Act only partially improve the current situation. The recently initialized "Umbrella Agreement" could lead to changes with regards to data protection guarantees in the law enforcement and national security sectors, but it remains to be seen which specific material rights and guarantees will be included in such an agreement. A leaked version of the Umbrella Agreement was published after the finalization of this study. A brief analysis of the agreement’s text is therefore added in the end.

1. SCOPE AND DEFINITIONS

The following study contains an in-depth analysis of general data protection principles in the law enforcement sector. It compares relevant US and EU data protection legislation in this specific area. Its purpose is to identify commonalities and divergences between the US and the EU approach to data protection in the law enforcement (LE) sector. The outcome of the study aims to serve as a basis for assessing the need for changes in law to safeguard privacy interests.

In the first comprehensive section, EU data protection provisions in the LE sector are analyzed. Starting with EU Primary Law, the basic rights and principles are presented. They can be found in the Treaty on the Functioning of the European Union and the Charter of Fundamental Rights of the European Union. Due to its importance regarding the development of data protection standards in the EU, relevant decisions of the European Court of Human Rights are also taken into consideration. Subsequently relevant EU Secondary Law is assessed, starting with a brief overview of the guarantees included in Directive 95/46/EC, Regulation 45/2001/EC, the proposed General Data Protection Regulation and the Directive for Data Protection in the Law Enforcement, before focusing on specific laws enacted with regard to law enforcement activities within the EU.

In the second section the most relevant US rules are examined. This part is based on the study "The US Legal System on Data Protection in the Field of Law Enforcement. Safeguards, Rights and Remedies for EU Citizens" by *Prof. Francesca Bignami*.[1] In line with the *Bignami* study, the analysis focuses on federal law enforcement and national security provisions while excluding laws on state and local level. More specifically, the general data protection principles derived from the Fourth Amendment to the US Constitution, the Privacy Act of 1974 and the safeguards established in connection with the laws empowering the law enforcement agencies to process data in order to comply with their tasks, are analysed. These safeguards can be found in the Electronic Communications Privacy Act, the Foreign Intelligence Surveillance Act, the Wiretap Act, the Stored Communications Act, the Pen Register Act or the USA PATRIOT Act. In order to present the evolution of privacy rights in the US, the new legislative actions that modify sections of the above mentioned Acts are analysed. The focus lies on the Draft Judicial Redress Act of 2015 and the FREEDOM Act of 2015. As the text of the "Umbrella Agreement" was not yet published at the time of writing the study, an assessment of its content could not been carried out.

At the end a brief comparison between the EU and the US data protection guarantees in the law enforcement and national security sector is carried out, based on the findings of the first two parts.

Some essential notions used in this study should be clarified beforehand.

The term law enforcement generally refers to activities of the agencies responsible for the prevention, detection and investigation of crime and the execution of criminal penalties. In order to comply with this duty, law enforcement authorities rely on the permission to be able to collect, use and disseminate personal data (process personal data). The extent to which data processing activities qualify as a law enforcement activity depends on the interpretation of "crime". The term can be used in a narrow or in a broad way. The content of crime may be limited to ordinary crime or include all forms of crime. The latter interpretation would explicitly encompass criminal activities that threaten national security.

[1] Bignami, The US legal system on data protection in the field of law enforcement. Safeguards, rights and remedies for EU citizens, Study for the LIBE Committee, PE 519.215, May 2015, available at: http://www.europarl.europa.eu/RegData/etudes/STUD/2015/519215/IPOL_STU%282015%29519215_EN.pdf.

The basis for the enactment of rules for the law enforcement sector within the European Union is Title V of the Treaty on the Functioning of the European Union. This title lays down the rules for the Area of Freedom, Security and Justice. The rules provide for *inter alia* judicial cooperation in criminal matters and police cooperation. However, it is noteworthy, that national security is excluded from this Area. According to Article 4 paragraph 2 of the Treaty of the European Union, national security remains the sole responsibility of each Member State. Consequently, the legal acts analysed in the framework of EU law do not contain data protection principles applicable in situations linked to national security threats. However this is different, when it comes to the analysis of the judgements made by the European Court of Human Rights, as this court has the authority to decide cases involving national security aspects.

The analyzed US legal provisions relate to both law enforcement and national security regulation, as data sharing between the agencies in these two fields is quite common. Data processed for law enforcement purposes may be used for criminal investigation, as well as for national security reasons by intelligence agencies, and vice versa. Consequently, the findings based on US law contain data protection principles which also apply when it comes to data processing connected to the protection of national security.

2. EU DATA PROTECTION GUARANTEES IN LAW ENFORCEMENT

2.1. EU Primary Law

Data protection guarantees exist at a primary law level since 2009, when the Lisbon Treaty came into force. Article 16 of the Treaty on the Functioning of the European Union (TFEU) explicitly refers to the individual right to data protection and lays down procedural rules for the legislative process in these matters.[2] Moreover, the Charter, which became binding at the same time, entails two provisions, namely Article 7 and 8 Charter of Fundamental Rights of the European Union (CFR) which assure privacy and data protection for "everyone".[3] The guarantees of both rights fall within the scope of EU law, including the LE sector (Title V TFEU, Area of Freedom, Security and Justice).

The application and interpretation of these rights resides with the Court of Justice of the European Union (CJEU). However, the Court has gained the competence to decide in law enforcement related cases with reference to EU law, only since the former pillar structure was abolished in 2009 with the Lisbon Treaty. This formerly restricted competence is also the reason for the limited existing case law within this specific context so far. Although, in the last few years the Court has seemed to become increasingly aware of its judicial powers in the LE sector. In April 2014, it delivered an important judgement for the LE sector with the complete and retrospective annulment of the Data Retention Directive 2006/24/EC (DRD).[4] This decision had significant consequences for the relationship between the rights to data protection and privacy on the one hand, and LE measures in the EU and its Member States on the other hand.[5] The principles developed in this case are crucial for the interpretation of Article 7 and 8 CFR in regards to EU data protection legislation for law enforcement purposes. These principles are discussed in this section. Firstly, a brief overview of the legal sources of data protection in primary law is given.

2.1.1. Article 16 TFEU

Article 16 TFEU mirrors the right to data protection established in Article 8 of the Charter. Read together with Article 39 TFEU[6], it stipulates the competences of the EU in data protection related matters and refers to the ordinary legislative procedure for the adoption of data protection rules at EU level in its second paragraph. The same paragraph entails not only procedural rules, but also relates to substantive data protection guarantees, in particular to the control of independent authorities, which is also referred to in Article 8 (3) CFR. Article 16 TFEU reads as follows:

> 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

[2] Consolidated version of the Treaty on the Functioning of the European Union, OJ C 326, 26.10.2012, p. 1 – 390 (in the following: TFEU).
[3] Charter of Fundamental Rights of the European Union, OJ C 83, 30.3.2010, p. 389 – 403 (in the following: CFR).
[4] CJEU, joined cases C-293/12 and C-594/12, *Digital Rights Ireland and Seitlinger and Others,* Judgment of the Court of 8 April 2014 (in the following: CJEU, C-293/12 and C-594/12 *Digital Rights Ireland*).
[5] Boehm/Cole, Data retention after the Judgement of the Court of Justice of the European Union, June 2014, the study was requested by the Greens/EFA Group in the European Parliament, it is available at: http://www.greens-efa.eu/data-retention-12640.html (in the following: Boehm/Cole, Data retention study).
[6] Article 39 TFEU provides for a particular legal process to adopt data protection rules in the field of the common foreign and security policy.

> 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.

By mentioning "everyone" in the first paragraph, the scope of the provision does not only include EU citizens, but all (natural) persons. Union institutions, bodies, offices, agencies and the Member States are obliged to respect the guarantees of Article 16 TFEU when processing personal data and carrying out activities, which fall within the scope of EU law. The term processing has a wide application and refers to the various forms of collection, storage and use of the data.[7] In accordance with the concept of the Lisbon Treaty, Article 16 TFEU refers to EU law and abolishes the former distinction between EC and EU law. As a consequence, the right to the protection of personal data applies equally to the former first pillar (internal market), as well as the former third pillar matters (LE). Though, two declarations (n° 20 and 21) annexed to the Lisbon Treaty state that legislation based on Article 16 TFEU, relating to the protection of personal data in the field of national security, judicial cooperation in criminal matters and police cooperation, may require the adoption of particular rules due to the specific characteristics of these issues. The two proposals for a general data protection regulation and the data protection directive in the LE sector follow this particular approach. The framework of the Common Foreign and Security Policy Article 39 TFEU lays down specific rules and authorizes the Council to adopt a decision regulating data protection rules with regard to this specific field of policy.

2.1.2. European Charter of Fundamental Rights

In addition to Article 16 TFEU, Articles 7 and 8 CFR are two further important sources of data protection at primary law level. Both articles establish two comprehensive rights protecting private life and personal data of individuals. The explicit mentioning of the specific data protection provision in the CFR distinguishes the Charter from the European Convention on Human Rights (ECHR) and emphasizes the significance of data protection as an important fundamental right within the framework of EU law. The guarantees stemming from these two articles are illustrated in detail in the following subsections.

2.1.2.1. Scope of application of Articles 7 and 8 of the Charter

The field of application of Article 7 and 8 CFR is determined by Article 51 CFR. According to its first paragraph, the provisions of the CFR are principally "addressed to the institutions, bodies, offices and agencies of the Union". The guarantees of the CFR also apply to the Member States, but "only when they are implementing Union law". Article 51 (2) CFR confirms that the provisions of the Charter do not extend beyond the field of EU law and are not capable of establishing new competences for the EU.

The Court has developed extensive case law on the question of the applicability of the CFR.[8] Recent judgements indicate a wide scope of application of the guarantees of the Charter. In the two cases of 2013, *Åkerberg Fransson* and *Melloni*, the Court stressed the

[7] Compare Article 2 (b) Directive 95/46/EC, OJ L 281, 23.11.1995, p. 31 – 50 (in the following: Directive 95/46/EC): "processing of personal data' ('processing') shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, 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".

[8] For instance: CJEU, Case C-279/09, *DEB Deutsch Energiehandels- und Beratungsgesellschaft mbH v Bundesrepublik Deutschland,* Judgement of the Court of 22 December 2010; CJEU, Case C-370/12, *Thomas Pringle v Government of Ireland, Ireland and The Attorney General*, Judgement of the Court of 27 November 2012; for more details see for instance: Ward, in: Peers/Hervey/Kenner/Ward, Article 51, pp. 1413 et seq.

broad interpretation of the Charter's scope.[9] In particular in *Åkerberg Fransson*, the Court emphasized that "… the fundamental rights guaranteed in the legal order of the European Union are applicable in all situations governed by European Union law".[10] The applicability includes the "… applicability of the fundamental rights guaranteed by the Charter".[11] Even in areas in which EU law only partially governs a case, Member States only maintain a discretion for the issue to be governed by national law, as long as they assure that "… the level of protection provided for by the Charter, as interpreted by the Court, and the primacy, unity and effectiveness of European Union law" are not compromised by such national rules.[12] The wording used by the Court can also be interpreted as having a very wide – if not a different – understanding of the term "implementation" as entailed in Article 51 (1) CFR. If an area is entirely governed by EU law, national law including the constitutional rules, are inapplicable if they are inconsistent with the Charter or undermine the effectiveness of EU law.[13] Both cases illustrate the extensive scope of application of the Charter's provisions covering all areas within the competence of EU law. As a consequence, in addition to the traditional Union policies of the former first pillar (internal market) such as free movement of persons, services and capital, the competences of the EU also incorporate Title V TFEU the "Area of Freedom, Security and Justice" and therefore include data protection in the LE sector.

2.1.2.2. Substantive guarantees of Article 7 and 8 of the Charter

Articles 7 and 8 CFR are two essential rights protecting private life and personal data of individuals. Both articles are intertwined and mirror Article 8 ECHR, in particular Article 7 CFR, which has a similar wording. Its scope includes the right to private and family life, home and communications. Article 8 CFR reaches even further by specifying a separate part on the right to private life and establishes a right to the protection of personal data. It is based on Article 8 ECHR, Article 286 EC Treaty, Directive 95/46/EC and Convention No. 108 of the Council of Europe.[14] These two provisions read as follows:

> Article 7: Respect for private and family life
>
> Everyone has the right to respect for his or her private and family life, home and communications.
>
> Article 8: Protection of personal data
>
> (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.

Article 7 CFR corresponds to the rights guaranteed by Article 8 ECHR and include the **concept of private life**. As the concept is very wide-ranging, there is no

[9] CJEU, Case C-617/10, *Åklagaren v Hans Åkerberg Fransson,* Judgment of the Court of 26 February 2013 (in the following: CJEU, C-617/10 *Åkerberg)*; CJEU, Case C-399/11, *Stefano Melloni v Ministeria Fiscal,* Judgment of the Court of 26 February 2013 (in the following: CJEU, C-399/11 *Melloni)*.
[10] CJEU, C-617/10 *Åkerberg*, para 19.
[11] CJEU, C-617/10 *Åkerberg*, para 21.
[12] CJEU, C-617/10 *Åkerberg*, para 29 and CJEU, C-399/11 *Melloni*, para 60.
[13] CJEU, C-399/11 *Melloni*, para 59.
[14] Kranenborg, in: Peers/Hervey/Kenner/Ward, Article 8, p. 223.

exhaustive definition of the notion of private life.[15] Its inclusive character allows it to cover various situations and activities that encompass this principle.

Article 8 CFR also covers a part of the private life guarantees by protecting personal data of individuals. Just as Article 7, it is to be consistently interpreted with Article 8 ECHR, including the aspect of private life. The Court summarizes the close relationship between Article 7 and 8 CFR as follows:

"… the right to respect for private life with regard to the processing of personal data, recognised by Articles 7 and 8 of the Charter, concerns any information relating to an identified or identifiable individual […] and the limitations which may lawfully be imposed on the right to the protection of personal data correspond to those tolerated in relation to Article 8 of the Convention [ECHR]."[16]

In addition to this broad definition, the Court recognized the retention and processing of data as belonging to Article 7 and 8 CFR.[17] Regarding its personal scope, both Articles refer to "everyone" and include therefore not only EU citizens, but all (natural) persons, whose rights, stemming from Article 7 and 8 CFR, have been infringed within the competence of EU law.[18]

In contrast to Article 7, Article 8 CFR entails some substantive guarantees regarding the content of the right to data protection. These principles are detailed in secondary law, in particular in Directive 95/46/EC and in the other instruments on which Article 8 CFR is based. Specifically mentioned in Article 8 (2) are the principles of purpose limitation, fair processing and processing on the basis of consent or another legitimate legal basis. Further rights mentioned in paragraph (2) include the rights of access and rectification. Another essential component, which was frequently subject to recent CJEU case law, is independent oversight. It is prominently stipulated in paragraph (3) of Article 8 CFR and it is also laid down in Articles 16 (2) and 39 TFEU.

Article 6 of Directive 95/46/EC refers to **purpose limitation** and specifies that data must be "collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes". This principle constitutes one of the key data protection guarantees as it intends to considerably limit the use of collected data. As with every rule, there are exceptions to this principle, but such exceptions are limited. The next principle which is mentioned refers to a fair processing of the data. This provision relates to a transparent and informative data collection and processing procedure. Data controllers can comply with this requirement by informing the data subject about the details of the data processing. A fair processing is therefore the pre-condition for invoking other rights, such as access, objections or rectification. Provisions on the information of the data subject can be found in Article 10 and 11 of Directive 95/46/EC. The data subject must be provided, for instance, with information about the identity of the controller and of his representative, the purposes of the processing for which the data are intended and if necessary further information, e.g. about the recipients or categories of recipients of the data.

[15] Compare for instance: ECtHR, *Niemietz v. Germany*, Application no. 13710/88, Judgment of 16 December 1992, paras 29 et seq.
[16] CJEU, joined cases C-92/09 and C-93/09, *Volker und Markus Schecke and Eifert*, Judgment of the Court of 9 November 2010 (in the following: CJEU, C-92/09 and C-93/09 *Schecke*), para 52.
[17] CJEU, C-293/12 and C-594/12 *Digital Rights Ireland*, para 29.
[18] Directive 95/46/EC exclusively refers to natural persons, whereas Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, OJ L 201, 31.07.2002, p. 37 – 47, also partly covers legal person in its Article 1 (2) as well as Article 13 (1).

A further requirement stated in Article 8 (2) CFR is the processing of data on the basis of **consent or another legitimate legal basis**. Legitimate grounds for processing are laid down in Article 7 of Directive 95/46/EC. The grounds stipulated in this list are exclusive and not extensible. Consent is the first ground mentioned and needs to be unambiguously given. It is further defined in Article 2 (h) of Directive 95/46/EC as meaning "… any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed".[19] The other grounds are processing necessary for the performance of a contract; or for compliance with a legal obligation to which the controller is subject; or in order to protect the vital interests of the data subject; or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; or for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except when such interests are overridden by the interests for fundamental rights and freedoms of the data subject.[20] Excluding consent as a legitimate basis, the data processing for all other mentioned grounds needs to be necessary, meaning that a balance between the different interests at stake needs to be met in each individual case.[21] The necessity concept has "its own independent meaning" in EU law and the CJEU is responsible for interpreting it within the framework of Directive 95/46/EC.[22]

The other rights mentioned in paragraph (2) include the **rights of access and rectification**. They complete the transparency aspect of fair processing and are equally detailed in Directive 95/46/EC. The data subject has the right to obtain disclosure from the controller without constraint at reasonable intervals and without excessive delay or expense confirmation as to whether or not his data are being processed and information at least in regards to the purposes of the processing, the categories of data concerned, and the recipients or categories of recipients to whom the data are disclosed.[23] This information has to be communicated to the data subject in an intelligible form including knowledge of the logic involved in any automatic processing of data, at least in the case of automated decisions.[24] The right to access enables an individual to understand what kind of data are stored and therefore constitutes an essential pre-condition for the enforcement of other rights, such as rectification, erasure and judicial redress. The right to access is inseparably linked to the past data processing and therefore includes an obligation for the controller to implement an appropriate and fairly balanced time limit for the storage of the information, which enables the individual to effectively invoke its access right.[25] For example, in *Rijkeboer* the Court considered a one year storage period for information on how the collected data has been used as being too short.[26] Regarding the other mentioned rights in the framework of access the Charter only mentions the right to rectification, which is also specified in Article 12 of Directive 95/46/EC. Its letter (b) establishes the

[19] Compare for details: Article 29 Data Protection Working Party, Opinion 15/2011, available at: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp187_en.pdf.
[20] Compare Article 7 (a) to (f) of Directive 95/46/EC.
[21] Compare for a necessity test with regard to the question whether a centralized register of foreign nationals was necessary in Germany: CJEU, Case C-524/06, *Heinz Huber v. Germany*, Judgment of the Court of 16 December 2008, paras 47 et seq (in the following: CJEU, C-524/06 *Huber*).
[22] CJEU, C-524/06 *Huber*, para 52.
[23] Article 12 (a) of Directive 95/46/EC.
[24] Article 12 (a) of Directive 95/46/EC.
[25] CJEU, Case C-553/07, *College van burgemeester en wethouders van Rotterdam v M. E. E. Rijkeboer,* Judgment of the Court of 7 May 2009 (in the following: CJEU, C-553/07 *Rijkeboer)*, para 54.
[26] CJEU, C-553/07 *Rijkeboer*, para 70.

right to rectification, if the processing of data does not comply with the provisions of Directive 95/46/EC, in particular because of incomplete or inaccurate data. The Directive adds the rights to erasure, blocking and objection to the essential rights of the individual. It is worth noting that the individual mentioning of the rectification right in the Charter does not indicate that the other rights are less important. The Charter, as an instrument of primary law, can evidently only refer exemplarily to some of the rights which are then specified in secondary law.

Finally, paragraph (3) of Article 8 CFR, like Articles 16 (2) and 39 TFEU, includes an essential component of EU data protection law by referring to **independent control of supervisory authorities**. Independent oversight is also mentioned in Recital 62 as well as Article 28 (1) of Directive 95/46/EC as being "an essential component" of data protection law. This view has already been confirmed three times by the CJEU, which refers to the supervisory authorities as "guardians of the right to private life" and considers independence as crucial for data protection.[27] In cases against Germany, Austria and Hungary, the Court clarified that the term independence refers to "complete independence", meaning the exercise of duties free from any external influence, whether direct or indirect.[28] Already the "mere risk" that states could exercise a political influence over the decisions of the supervisory authorities was enough to violate EU law.[29] In the Hungarian case, the premature ending of the term served by the supervisory authority contradicted Article 28 of Directive 95/45/EC.[30] The CJEU therefore applies very strict criteria when it comes to the interpretation of the term independency. The powers of investigation, intervention and engagement in legal proceedings are further functions and competences of supervisory authorities which are additionally specified in Article 28 of Directive 95/46/EC.

Summarizing, the Charter entails important substantive data protection guarantees, which are, however, only a starting point for a much elaborated data protection system developed in secondary law.[31] This secondary legislation has to comply with the elements stipulated in the Charter and could, in case of conflict, as seen in the data retention case, be declared invalid by the CJEU. These conflicts mostly arise due to the fact that the existing instruments in secondary law still reflect the pre-Lisbon situation. The Charter, creates an overarching framework for all policy areas, including LE, and raises the guarantees mentioned in Article 8 CFR to a primary law level, creating a direct effect.[32] The key elements mentioned in Articles 7 and 8 CFR are therefore also applicable in the LE sector.

2.1.2.3. Limitations to the rights of Article 7 and 8 CFR

When Articles 7 and 8 CFR apply to a special context, as established by Article 51 CFR, rules on the interpretation of these fundamental rights and freedoms of the Charter can be found in Article 52 CFR.[33] In its paragraph (1), the same article lays down rules for the

[27] CJEU, Case C-518/07, *Commission v. Germany*, Judgment of the Court of 9 March 2010 (in the following: CJEU, C-518/07 *Commission v. Germany)*, paras 23 and 36; Case C-614/10, *Commission v. Austria*, Judgment of the Court of October 2012 (in the following: CJEU, C-614/10 *Commission v. Austria*), para 37; Case C-288/12, *Commission v. Hungary*, Judgment of the Court of 8 April 2014 (in the following: CJEU, C-288/12 *Commission v. Hungary*), para 48.
[28] CJEU, C-518/07 *Commission v. Germany*, para 30.
[29] CJEU, C-518/07 *Commission v. Germany*, para 36.
[30] CJEU, C-288/12 *Commission v. Hungary*, para 62.
[31] Compare for a comprehensive overview: Kranenborg, in: Peers/Hervey/Kenner/Ward, Article 8, pp. 223 et seq., in particular 265.
[32] Kranenborg, in: Peers/Hervey/Kenner/Ward, Article 8, p. 240.
[33] For details see: Peers/Prechal, in: Peers/Hervey/Kenner/Ward, Article 52, pp. 1455 et seq.

possible limitation of rights. The provision codifies long established case law of the Court and has a similar wording and meaning as the limitations and derogations provided for the rights of the ECHR, which was, in addition to national constitutions, the principal source of inspiration for the EU fundamental rights.[34] Relatively often these principles were used and developed in data protection related cases by the Court.[35]

Article 52 (1) CFR firstly contains a procedural rule by stressing that restrictions to the rights of the Charter need to be provided for by law. Additionally, from a substantive point of view, limitations must respect the essence of those rights. Furthermore, any restrictions are subject to the principle of proportionality, meaning that they must be necessary and genuinely meet the objectives of general interest of the Union or are needed to protect the rights and freedoms of others.[36] When verifying whether a limitation is substantively justified and sufficiently balanced to be in accordance with the Charter, the Court usually applies a three-step test: firstly, it answers the question as to whether the essence of the rights are respected, secondly, whether the measure at stake meets the objective of general interest and lastly, whether the boundaries of proportionality, specifically appropriateness and necessity are met.[37] Obviously, if already the procedural requirement, namely that a restriction is "provided for by law", is not complied with, there is no need to apply the three-step justification test.[38] Similarly to the ECtHR, the Court usually focuses on the third aspect of necessity and by doing so balances the opposing interests against each other.

In an LE context, Article 7 and 8 of the Charter may therefore be lawfully restricted. For instance, the Court has already recognized, amongst others, the fight against serious crime in order to ensure public security, the fight against international terrorism in order to maintain international peace as well as the prevention of illegal entry into the EU as objectives of general interest.[39] Special attention has to be paid to ongoing investigations in an LE context, which may be undermined, if, for instance, the data subject is informed about the investigation or has access to its data stored in this framework. However, all restrictions need to pass the three-step test and must comply with the strict requirements of Article 52 (1) CFR as mentioned above.

2.1.2.4. The specific case of data protection in the LE sector

The interplay between the Court's case law, the CFR and the guarantees developed by the ECtHR with regard to the ECHR are particularly visible in data protection related cases. When data protection issues were the subject of EU cases, and before the EU was officially requested to accede to the ECHR (Article 6 (2) TEU) and before the EU Treaties explicitly mentioned Fundamental Rights, the Court referred to the guarantees developed with regard to Article 8 ECHR. In *Roquette Frères*, the Court specified that the ECtHR's case law on Article 8 (2) ECHR had to be taken into account when deciding on the lawfulness of an investigation into private business premises.[40] More prominently, the Court interpreted

[34] Peers/Prechal, in: Peers/Hervey/Kenner/Ward, Article 52, pp. 1455 et seq.
[35] For instance in: CJEU, C-92/09 and C-93/09 *Schecke*; CJEU, Case C-70/10, *Scarlet Extended*, Judgment of the Court of 24 November 2011 (both cases in particular with regard to the justification test) and CJEU, C-293/12 and C-594/12 *Digital Rights Ireland* (with regard to the essence of rights).
[36] Article 52 (1) CFR.
[37] Compare: CJEU, C-293/12 and C-594/12 *Digital Rights Ireland*, earlier: CJEU, C-92/09 and C-93/09 *Schecke*.
[38] Peers/Prechal, in: Peers/Hervey/Kenner/Ward, Article 52, pp. 1455 et seq., in particular p. 1480.
[39] In this order: CJEU, C-293/12 and C-594/12 *Digital Rights Ireland*, para 42; CJEU, Joined cases C-402/05 P and C-415/05 P, *Kadi and Al Barakaat International Foundation* v *Council and Commission*, Judgment of the Court of 3 September 2008, para 363; Case C-291/12, *Schwarz*, Judgment of the Court of 17 October 2013 (in the following: CJEU, C-291/12 *Schwarz*), para 37.
[40] CJEU, Case C-94/00 *Roquette Frères*, Judgment of the Court of 22 October 2002, para 29; compare also the joined Cases C-238/99P, C-244/99P, C-245/99P, C-247/99P, C-250/99P to C-252/99P and C-254/99P, *Limburgse Vinyl Maatschappij and Others v Commission,* Judgment of the Court of 15 October 2002.

Directive 95/46/EC in light of Article 8 and 10 ECHR in the cases *Österreichischer Rundfunk* and *Lindqvist*.[41] In particular, in examining the existence and justification of an interference with Directive 95/46/EC, the Court applied standards developed by the ECtHR. As both courts focus on the aspect of necessity, the justification test – which was then codified in Article 52 (1) CFR – was applied exemplarily in cases, such as *Volker and Schecke*, *Scarlet Extended* and the *Data Retention* case.[42]

Today, Article 6 TEU declares the CFR to have the same value as the Treaties and requests an accession of the EU to the ECHR. According to Article 6 (3) TEU, the fundamental rights of the ECHR "shall constitute general principles of the Union's law". Moreover, Article 52 (3) CFR stresses that for rights, which correspond to the rights of the ECHR "the meaning and scope of those rights shall be the same as those laid down in the Convention". The ECtHR's case law based on Article 8 is therefore not only an important source, but entails guiding principles for the interpretation of Articles 7 and 8 of the Charter.

The close link between the EU and the Strasbourg Court is of particular importance in the field of data protection in the LE sector. Until the Lisbon Treaty entered into force in 2009, the CJEU had no competence to decide in LE related matters, as this specific field of policy was part of the former third pillar and was excluded from its scope of jurisdiction. Therefore in the past important data protection guarantees in the LE sector were often developed by the ECtHR. The principles developed in this context are illustrated below in section 2.3.1. Although, since these cases are being submitted to the CJEU to a much greater extent than ever before, this rather unilateral allocation of tasks is beginning to change.

2.1.3. EU-Case Law

The limited competence of the CJEU, with regard to former third pillar matters before the Lisbon Treaty was adopted, is the reason for the limited amount of EU cases dealing with data protection in the LE sector so far. The non-binding nature of the Charter at the time may be a further explanation for the hesitant approach of the CJEU to deal with questions that arose in relation to this sensitive context.

The few cases that touched upon the LE environment prior to 2009 mainly concerned conflicts over the competence of the EU to pass legislative acts in an LE environment, in particular in the field of Passenger Name Records (PNR) and data retention. It is important to note that in both cases, the CJEU refrained from answering questions of substantial nature, possibly due to the reasons mentioned above. Since 2009, cases including LE aspects, began to frequently increase. Undoubtedly, the most important LE case of the CJEU is the recently decided annulation of the Data Retention Directive.

2.1.3.1. First PNR and Data Retention cases

The first cases in the field of LE before the CJEU involved the choice of the legal basis for the (first) PNR agreement with the US and the recently annulled Data Retention Directive 2006/24/EC.[43] Both instruments were initially adopted under the first pillar legal framework

[41] CJEU, joined Cases C-465/00, C-138/01 and C-139/01, *Österreichischer Rundfunk and Others*, Judgment of the Court of 20 May 2003, paras 73 et seq; CJEU, Case C-101/01, *Lindqvist*, Judgment of the Court of 6 November 2003, paras 76 et seq.
[42] CJEU, C-92/09 and C-93/09 *Schecke*; CJEU, Case C-70/10, *Scarlet Extended*, Judgment of the Court of 24 November 2011 (both cases in particular with regard to the justification test); CJEU, C-293/12 and C-594/12 *Digital Rights Ireland* (with regard to the essence of rights).
[43] CJEU, Joined cases C-317/04 and C-318/04, *Parliament v. Council*, Judgment of the Court of 30 May 2006; Case C-301/06, *Ireland v. Parliament and Council,* Judgment of the Court of 10 February 2009.

(internal market) of the EC Treaty.[44] Due to the LE related context of these measures, this choice was questioned and the Court had to decide whether a third pillar legal basis (LE) would have been the better choice. The Court reached two different solutions in 2006 and February of 2009. The US-PNR agreement should have been based on an LE legal basis whereas the first pillar choice of the Data Retention Directive constituted the correct legal basis. The reasons for the different treatment of such similar measures are not necessarily obvious. The Court based its arguments mainly on the fact that the Data Retention Directive did not entail rules on the use and the access procedure for LE to the stored data, while the PNR agreement did. One possible explanation for this rather artificial distinction relates to the consequence which a ruling requiring a third pillar choice for the Data Retention Directive would have had. If the Court had annulled the first pillar choice, any measure concerning data retention on the EU level, which was used for LE purposes, would have had to be based on a third pillar option.[45] This would have excluded both European Parliament and European Data Protection Supervisor from the legislative process and would have hindered any direct control over such sensitive matters. It is also worth noting that the Court refrained from examining any fundamental rights related questions, although in particular in the PNR case, the applicants challenged this issue.

Both cases illustrate the hesitant approach of the Court to deal with substantive fundamental rights questions in LE related matters before the Lisbon Treaty was adopted. Therefore, although these cases concern important questions in the LE area, the judicial assessment of such questions had to wait until the Court was sufficiently empowered under the framework of the Lisbon Treaty to answer them.

2.1.3.2. Schwarz, C-291/12, taking of fingerprints in passports

One of the first cases partly dealing with data protection in the LE sector after the adoption of the Lisbon Treaty was the Schwarz case in 2013, which concerned the storing and subsequent use of fingerprint records in passports.[46] Council Regulation 2252/2004 established harmonized security features for EU-passports requiring Member States to include two fingerprints in travel and passport documents.[47] Mr. Schwarz, a German citizen, applied for a passport, but refused to be fingerprinted. He argued that the obligation to be fingerprinted constituted a gross violation of his rights stemming from Article 7 and 8 of the Charter. While the Court found that fingerprint records certainly constitute personal data and that the taking and storing of those fingerprints amounted to an interference with Article 7 and 8 CFR, it did not find a violation of those rights. Clearly, the judgement itself is not a very prominent case, which is presumably due to the rather unusual arguments used by the Court to come to this conclusion, but it should be mentioned to obtain a complete picture of the case law in LE matters.

In *Schwarz*, the Court recognized for the first time the prevention of illegal entry into the EU as an objective of general interest.[48] It further argued that the taking of fingerprints is always visible to others and is therefore "… not an operation of an intimate nature", nor "does it cause any particular physical or mental discomfort to the person affected …".[49] This is obviously true, but in view of typical data protection cases, these arguments are of little help as in most of these situations there is no direct or physical harm involved. This

[44] For more details, compare: Boehm, in: Privacy and Data Protection, An Element of Choice, Chapter 8, pp. 171-191.
[45] Boehm/Cole, Data retention study, p. 14.
[46] CJEU, C-291/12 *Schwarz*.
[47] Article 1 Council Regulation (EC) No 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States, OJ L 385, 29.12.2004, p. 1 – 6.
[48] CJEU, C-291/12 *Schwarz*, para 37.
[49] CJEU, C-291/12 *Schwarz*, para 48.

missing "immediate effect" of nonetheless infringing measures is one of the difficulties the enforcement of data protection rules characteristically face. Regrettably, this argument went unnoticed by the Court. Nevertheless, it was corrected in the subsequent data retention case.[50] Instead, the Court continued with a very brief analysis of the provisions of the regulation and decided not to discuss the risk resulting from the storage of fingerprint records, avoiding a discussion of the consequences the continued storing of such data, possibly in a central database at Member State level, could have. The CJEU came to the conclusion that Council Regulation 2252/2004 was in accordance with Articles 7 and 8, in particular, as it did not provide for the establishment of a centralized storing facility for fingerprint data, but only for the storing of the data within the passport, which, according to the Court, "belongs to the holder alone".[51] The possibility of a centralized database was not specifically regulated by the regulation, but it was also not excluded. Therefore the Court did not feel authorized to decide on this question.

Possibly, due to the rather unusual legal reasoning of the Court in the *Schwarz* case and the restricted scope of the issue, this judgement is rarely referred to and mostly ignored in later decisions. However, it is not excluded that the Court in a possible case concerning border protection, comes back to the thoughts stated in this case. It is then rather questionable, whether the risks of data storing could be ignored to the same extent as the Court did in the *Schwarz* case. The data retention case, decided only one year later and discussed in the next section, demonstrates an increasing understanding of the risks of legal rules providing for the storage of huge amounts of personal records in large databases.

2.1.3.3. 2nd data retention case

After the rather unspectacular *Schwarz* case, the Court finally delivered a key judgement for data protection and privacy in the LE sector in April 2014.[52] The background of the judgement is a joined case based on two preliminary rulings submitted by the Irish High Court and the Austrian Constitutional Court.[53] The applicant in the Irish case was the NGO "Digital Rights Ireland" and the referring High Court asked a series of questions relating to the fundamental rights compatibility. The Austrian case originates in a "class action" brought by more than 11.000 Austrian Citizens against parts of the national telecommunications law transposing the Data Retention Directive.[54]

By entirely and retrospectively annulling the Data Retention Directive, the Court stressed the seriousness of the directive's violation of fundamental rights, which had been in place since 2006. During the first case concerning this directive in 2009, the Court did not touch upon fundamental rights issues, but in the second data retention case, it detailed the directive's provisions by analyzing its consequences for the rights stipulated in Articles 7 and 8 CFR.

The judgement has **three major consequences**: Firstly, the Court opposes general and undifferentiated data retention measures for LE purposes and establishes important principles that will determine future data protection and privacy rights in the LE sector. Secondly, it regularly refers to the guarantees of the ECHR and its interpretation in the ECtHR case law in the context of data retention measures, irreversibly linking the two legal orders and opening the possibility for a consistent interpretation of Article 8 ECHR and

[50] CJEU, C-293/12 and C-594/12 *Digital Rights Ireland*, para 33.
[51] CJEU, C-291/12 *Schwarz*, paras 58 et seq.
[52] CJEU, C-293/12 and C-594/12 *Digital Rights Ireland*, for a detailed analysis, compare: Boehm/Cole, Data retention study; Granger/Irion, European Law Review, Issue 6, 2014.
[53] Further details on the originating cases can be found in Cole/Boehm, CritQ (2014), 58, pp. 71 et seq.
[54] CJEU, C-293/12 and C-594/12 *Digital Rights Ireland*.

Article 7 and 8 CFR. Particularly mentioned are the cases *Leander v. Sweden, Rotaru v. Romania*, *Weber and Saravia v. Germany*, *Liberty and Others v. United Kingdom*, S*. and Marper v. United Kingdom* and *M.K. v. France*.[55] The cases *S. and Marper v. United Kingdom and M.K. v. France*, are of specific importance since the facts and circumstances of these cases are similar to the data retention situation and are concerned with the mass collection and storage of data for LE purposes. Therefore, the statements of the Court not only refer to the singular case of the DRD, but also establish general principles for similar data retention measures. Thirdly, the Court makes important comments on the essence of the rights to data protection and privacy in the LE framework. These statements are of particular importance in situations in which LE authorities intend to access content of personal data.

The **principles developed by the Court** are briefly summarized in the following.

Regarding the scope of Article 7 and 8 CFR, the Court explains "that it does not matter whether the information on the private lives concerned is sensitive or whether the persons concerned have been inconvenienced in any way".[56] This statement contradicts the arguments of the *Schwarz* case by clarifying that infringements in data protection cases are independent of personal discomfort of the persons affected. Moreover, the categories of data do no play a role when deciding about infringements with the rights laid down in Articles 7 and 8 CFR. Although the relevance of both articles in the data retention context is obvious, the Court derives the applicability of right to private life (Article 7 CFR) from the retention and possible access to data by LE authorities. As the retention also constitutes processing, Article 8 of the Charter is correspondingly affected.[57]

Important statements further concern the **scope and notion of interference**. By referring to ECtHR cases, the Court stipulates that the collection and retention of data, as well as the possibility of access by LE authorities each constitute separate infringements of Articles 7 and 8 CFR, which require a strict necessity and proportionality test.[58] The interferences caused by the DRD are assessed as "particularly serious" and "wide-ranging" as the data retention targets almost every EU citizens and results in a huge amount of retained data.[59] The interference was further qualified as being "likely to generate in the minds of the persons concerned the feeling that their private lives are the subject of constant surveillance".[60]

Having established an interference with Articles 7 and 8 CFR, the Court proceeds with the analysis of the **justification test** under Article 52 (1), thereby focusing on proportionality aspects. First, the Court declared that the **essence of the rights** are respected, although the infringements are considered as being particularly serious. Within the framework of Article 7 CFR, it was essential that the content of communication was not stored or accessed. Concerning the respect of the essence of rights of Article 8 CFR, the Court argued that certain data protection and security principles for providers are foreseen, which satisfy the minimum requirements and thus respect the essence of this right. These observations of the Court are important, not only because it was the first time that the Court made comments on the essence of Articles 7 and 8 CFR, but also because these principles are

[55] Compare CJEU, C-293/12 and C-594/12 *Digital Rights Ireland*, paras 35, 47, 54 and 55.
[56] CJEU, C-293/12 and C-594/12 *Digital Rights Ireland*, para 33.
[57] CJEU, C-293/12 and C-594/12 *Digital Rights Ireland*, para 29.
[58] CJEU, C-293/12 and C-594/12 *Digital Rights Ireland*, para 35.
[59] CJEU, C-293/12 and C-594/12 *Digital Rights Ireland*, para 37.
[60] CJEU, C-293/12 and C-594/12 *Digital Rights Ireland*, para 37.

essential in situations in which data, including content, are stored and transferred to other countries, where they are then accessed by LE authorities.[61]

The Court further considers data retention as contributing to an **objective of general interest**, namely to the fight against serious crime in order to ensure public security.[62] However, the concrete implementation of this objective of general interest needs to pass the proportionality test. With repeated reference to the ECtHR case law, this test is carefully carried out by the Court. It notes that due to the seriousness of the interference, the discretion of the EU legislature is limited, which requires a **strict proportionality and necessity test**.[63] In particular, because the DRD entails an "interference with the fundamental rights of practically the entire European population".[64]

With reference to the ECtHR cases *Marper v. United Kingdom* and *M.K. v. France*, the Court highlights the "significant risk of unlawful access to those data" and notes that the DRD covers "in a generalised manner, all persons and all means of electronic communication as well as all traffic data without any differentiation, limitation or exception."[65] It clearly opposes this form of **blanket and indiscriminate mass retention of data** and made further important comments on the fact that typically **unsuspicious individuals** are affected by this measure.[66] It also criticizes that no exceptions are provided for in the DRD, e.g. with regard to the protection of professional secrecy.

Another very important aspect in the case concerns the general situation in which data originally collected for other purposes are later used for LE purposes. The Court requires a **link between a threat to public security and the data retained for LE purposes**.[67] This link is of particular importance in an LE context, as it significantly influences the relationship between private and public actors, meaning that LE is only allowed to access data which has been collected for other purposes in individual cases. This aspect is not only relevant in the specific DRD case, but in every situation in which LE requires access to private sector data (such as PNR or SWIFT) or data originally collected for other purposes (e.g. Eurodac).

Further, the Court **opposes indefinite or even lengthy retention period of data retained**.[68] It criticized that no "objective criteria" for the determination of the storage period exist. The lack of limitations regarding the access of LE authorities to the retained data was also harshly criticized. A general reference to "serious crime" as a reason to access is not considered as sufficient by the Court.[69] The Court explicitly demands effective procedural rules such as **independent oversight** and access control by a court or another independent authority to limit the access to what is strictly necessary.[70] Also "the number of persons authorised to access and subsequently use" the data was missing and was therefore criticized by the Court.[71]

[61] Compare Section 2.2.4.
[62] CJEU, C-293/12 and C-594/12 *Digital Rights Ireland*, paras 41 et seq.
[63] CJEU, C-293/12 and C-594/12 *Digital Rights Ireland*, paras 45 et seq.
[64] CJEU, C-293/12 and C-594/12 *Digital Rights Ireland*, para 56.
[65] CJEU, C-293/12 and C-594/12 *Digital Rights Ireland*, paras 55 and 57.
[66] CJEU, C-293/12 and C-594/12 *Digital Rights Ireland*, para 58: "It therefore applies even to persons for whom there is no evidence capable of suggesting that their conduct might have a link, even an indirect or remote one, with serious crime."
[67] CJEU, C-293/12 and C-594/12 *Digital Rights Ireland*, para 59.
[68] CJEU, C-293/12 and C-594/12 *Digital Rights Ireland*, paras 59, 63 et seq.
[69] CJEU, C-293/12 and C-594/12 *Digital Rights Ireland*, para 60.
[70] CJEU, C-293/12 and C-594/12 *Digital Rights Ireland*, para 62.
[71] CJEU, C-293/12 and C-594/12 *Digital Rights Ireland*, para 62.

Another point of criticism refers to the **missing rules on data security and organizational measures** for private actors.[72] Instead the DRD permitted the providers to consider economic and financial aspects when implementing such measures and failed to fix a time-limit for the irreversible destruction of the data.[73] These aspects must be seen in the broader context of the delegation of retention powers to private actors, which is seen rather critically by the Court. Evidently, if private actors are allowed to consider financial aspects when determining the level of data security, this can lead to the implementation of lower security standards. Final remarks of the Court relate to the problem of **location of the stored data**. The DRD did not require the data to be stored within the EU.[74] Yet this, was found to be essential by the Court, as Article 8 (3) refers to the requirement of independent supervision, which cannot be fully assured when storing data abroad.

Even a brief reading of the case shows the Court's disappointment about the EU legislator having adopted an instrument infringing so fundamentally the rights of the Charter. It is therefore logical that the directive was declared invalid in its entirety, without any possibility for corrections or an interim period for review. The total invalidation of an EU instrument occurs rarely and highlights the Court's indignation regarding the provisions of the DRD. More generally, the principles developed in the case set standards for the constitutional limits of Articles 7 and 8 of the Charter. The case is therefore a landmark decision with far reaching consequences for LE measures in the EU. Based on this ruling, some Member States began to change their national data retention schemes. The most prominent example is perhaps the UK, which enacted the Data Retention and Investigatory Powers Act (DRIPA) in an emergency procedure very shortly after the judgement. However, this act was declared invalid by the Divisional Court of the UK recently, which based its line of arguments on the Court's DRD case.[75]

2.1.3.4. Google v. Spain

Although this case is not directly linked to an LE context, being mainly associated with the Court's recognition of the so-called "right to be forgotten" as a particular facet of a data subject's fundamental rights to the protection of those data and to privacy[76], it may nevertheless serve as a valuable guidance in respect to the Court's approach towards a profiling effect of information compiled in search results.

In short, the Court recognizes that an individual should have the possibility to request the removal of links in Google's search engine regarding its own personal information, even if such information is correct, because the applicant's right to privacy with respect to the processing of its personal data carried out by the search engine is considered paramount to Google's mere economic interests at stake.

In its findings, the Court also recognizes that "the organization and aggregation of information published on the internet that are effected by search engines with the aim of facilitating their users' access to that information may, when users carry out their search on the basis of an individual's name, result in them obtaining through the list of results a structured overview of the information relating to that individual that can be found on the

[72] CJEU, C-293/12 and C-594/12 *Digital Rights Ireland*, para 66.
[73] CJEU, C-293/12 and C-594/12 *Digital Rights Ireland*, para 67.
[74] CJEU, C-293/12 and C-594/12 *Digital Rights Ireland*, para 68.
[75] Compare: Davis Judgement, [2015] EWHC 2092 (Admin), Case No: CO/3665/2014, available at: https://www.judiciary.gov.uk/wp-content/uploads/2015/07/davis_judgment.pdf.
[76] Boehme-Neßler, NVwZ (2014) 825, p. 826.

internet *enabling them to establish a more or less detailed profile of the data subject*."[77] It explicitly finds that "the activity of a search engine is therefore liable to affect significantly, and additionally compared with that of the publishers of websites, the fundamental rights to privacy and to the protection of personal data…".[78]

The Court hereby implicitly acknowledges that a compilation of personal data in a personalized profile gives rise to a significant interference with the fundamental rights to the protection of data and to privacy. This may also have an impact in the LE context, when balancing legitimate public LE interest in establishing profiles against the fundamental rights of individuals.

2.1.3.5. LE cases to be decided in the near future

In addition to the data retention judgement, there are further cases in the LE sector which will be decided in the near future. They should be briefly mentioned here to complete the picture and keep track of current developments.

In *Schrems v. Data Protection Commissioner*, the Court is faced with the question whether the safe harbor decision allowing the transfer of Facebook data of EU citizens to the US, where these data are in fact accessed by US LE and secret service authorities, is still in accordance with EU fundamental rights.[79] The Advocate General's opinion was delivered on the 23rd of September, 2015.[80] He proposed that the Commission's Safe Harbor Decision should be declared invalid and even referred to a possible violation of the essence of the rights enshrined in Article 7 of the Charter through the US intelligence services accessing the content of data transferred.[81] As this opinion was delivered after this study was initially finalized, a detailed analysis of this opinion could not be carried out, but it is worth mentioning that the Court's decision in the *Schrems* case will have a considerable influence on the framework for future data exchanges between the EU and the US.

Directly linked to the implementation of data retention measures is the case *Tele2 Sverige v. Post- och telestyrelsen*.[82] The referring Swedish court asks the essential question that was not answered by the Court in the DRD case, specifically whether there "is a general obligation to retain traffic data covering all persons, all means of electronic communication and all traffic data without any distinctions, limitations or exceptions for the purpose of combating crime compatible with Article 15(1) of Directive 2002/58/EC, taking account of Articles 7, 8 and 15(1) of the Charter?". If the answer of the CJEU is negative, the Swedish court asked more concrete and specific questions to the Swedish data retention law in place. So far, no proceedings have taken place. Thus, the answer of the Court is expected

[77] CJEU, Case C-131/12 *Google Spain and Google v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*, Judgment of the Court of 13 May 2014 (in the following: CJEU, C-131/12 *Google Spain*), para. 37 (emphasis added).
[78] CJEU, C-131/12 *Google Spain,* para. 38.
[79] CJEU, Case C-362/14, *Schrems v. Data Protection Commissioner,* Reference for a preliminary ruling form High Court of Ireland made on 25 July 2014 (in the following: CJEU, C-362/14 *Schrems*); compare also: Boehm, Legal opinion on the adequacy of the safe harbor decision, available at: http://www.europe-v-facebook.org/CJEU_boehm.pdf (in the following: Boehm, Legal opinion on the adequacy of the safe harbor decision).
[80] Compare, press release: http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-09/cp150106en.pdf%20 and opinion, available at: CJEU, C-362/14 *Schrems*, opinion of 23rd of September, available at: http://curia.europa.eu/juris/document/document.jsf?text=&docid=168421&pageIndex=0&doclang=en&mode=req&dir=&occ=first&part=1&cid=518391.
[81] CJEU, Case C-362/14, *Schrems v. Data Protection Commissioner,* Opinion of the Advocate General Bot on 23rd of September 2015, para 177.
[82] CJEU, Case C-203/15, *Tele2 Sverige AB v Post- och telestyrelsen,* Request for a preliminary ruling from the Kammarrätten i Stockholm lodged on 4 May 2015.

to add clarity to the question whether the only remaining provision in EU law (Article 15 (1) of Directive 2002/58/EC) which still allows for data retention, complies with the Charter.

2.2. EU Secondary Law

Almost six years after the adoption of the Lisbon Treaty, the existing legislative framework in data protection matters in the EU still corresponds to the former pillar structure that made a distinction between the adoption of legislative proposals within the framework of the former first and the former third pillar. Whereas in the scope of EC law within the first pillar, the European Parliament had real participation rights, these rights were reduced to a mere consultation right with regard to the former third pillar legislative framework, which now corresponds mainly to Title V of the TFEU (Area of Freedom, Security and Justice). As a consequence, several legal acts regulating data protection in secondary law exist. Each of these acts has its particular scope of application and entails specific rights varying in its intensity of protection for individuals. The pillar heritage is also the reason for the non-applicability of the main piece of EU data protection, Directive 95/46/EC, to LE related data processing. Though, its values represent core data protection standards within the EU and it is hence being used as an importance framework of reference also in the LE sector.

Before the Lisbon treaty was adopted, even the first pillar EC law did not entail a special legal basis for the adoption of data protection rules. EC secondary data protection law is therefore based on the general harmonization clause for the internal market, namely Article 95 EC Treaty (today Article 114 TFEU). The intention of **Directive 95/46/EC** is therefore twofold: it protects the individual data protection rights as well as the free movement of personal data.[83] As mentioned, it excludes LE data processing from its scope. Such as the Directive 95/46/EC, the so called E-Privacy Directive, **Directive 2002/58/EC** on privacy and electronic communications is equally based on Article 95 EC. The third directive adopted on the basis of the harmonization clause was the Data Retention Directive, which was declared void in April 2014 by the CJEU.[84] The first pillar protection was completed by **Regulation 45/2001/EC** that includes data protection rules for the Community institutions and bodies. Primarily, this instrument mirrors the rules of Directive 95/46/EC for the EC institutional framework.[85]

Data processing rules in the former third pillar, todays Area of Freedom, Security and Justice, are sector-specific and are all based on Article 30 (1) (b) of the (former) EU Treaty (replaced today by Articles 87 and 88 TFEU). They include special provisions for former third pillar bodies such as **Europol** and **Eurojust,** or established rules for databases and data exchange mechanisms, such as the **Prüm decision**, the **Schengen Information System** (SIS), **Eurodac** or the **Visa-Information System**.[86] Most of these decisions are now in a review process and are planned to be or are already adopted under the Lisbon framework. A more general instrument within the third pillar framework is **Framework Decision 2008/977/JHA,** which was adopted in 2008.[87] Although this instrument intends to establish overarching data processing rules for the EU LE area, it excludes the specific

[83] Article 1 of Directive 95/46/EC.
[84] Compare above, section 2.1.3.3.
[85] Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 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, OJ L 8, 12.1.2001, p. 1 – 22 (in the following: Regulation 45/2001) based on Article 286 EC Treaty.
[86] OJ L 121, 15.5.2009, p. 37 – 66 (Europol); OJ L 183, 4.6.2009, p. 14 – 32 (Eurojust); OJ L 210, 6.8.2008, p. 1 – 11 (Prüm); OJ L 239, 22.9.2000, p. 19 – 62 (Schengen); OJ L 316, 15.12.2000, p. 1 – 10 (Eurodac); OJ L 218, 13.8.2008, p. 60 – 81 (VIS).
[87] Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, OJ L 350, 30.12.2008, p. 60–71 (in the following: Framework Decision 2008/977/JHA).

rules for EU bodies and databases as well as domestic data processing from its scope, restricting its application to data processing rules regarding cross-border activities of Member States.

The entry into force of the Lisbon Treaty changed the EU's constitutional architecture, creating a specific legal basis with Article 16 TFEU for the adoption of a comprehensive data protection framework covering former first as well as third pillar policy areas. However, the instruments proposed on this basis in 2012 still mirror the former division into different policies. A **General Data Protection Regulation** (GDPR)[88] to replace Directive 95/46/EC and a separate **Directive for Data Protection in the LE sector** (DDPLE)[89] to replace Framework Decision 2008/977/JHA are being planned. These instruments nonetheless represent a more comprehensive approach covering, for instance, also domestic LE data processing. The regulation would at least replace national data protection laws, thereby creating harmonized and directly applicable rules for controllers and processors as well as protecting individuals rights in the EU. As stipulated in all already existing instruments mentioned above, the individual rights specified in these instruments apply to individuals subjected to the legislation of Member States, independent of a status as an EU citizen.

In view of this patchwork of data protection instruments, deriving **common EU principles for data protection in the LE sector** from these instruments is a difficult task, in particular, as the GDPR and the DDPLE are still in the negotiation process. Negotiations on the GDPR are, however, further advanced than the DDPLE legislative process. In June, the Council reached a general approach in preparation for the trilogue meetings.[90] With regard to the DDPLE, it seems that Member States prefer to wait for a common position on the GDPR provisions before deciding on the details of the DDPLE. For the purpose of this study, the most recent versions of these instruments have been considered; references are made to former versions, if required.[91] In spite of the intermediary stage as well as the existing legal patchwork, the following analysis makes the attempt to illustrate common principles for data protection in LE which can be found in almost all of the mentioned instruments, referring to the respective instruments in place, where necessary.

2.2.1. Quality Standards

All EU data protection instruments independent of the policy area contain standards relating to the quality of data including the requirements on a **fair and lawful processing**,

[88] 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(2012) 11 final (in the following: GDPR).
[89] 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, Com(2012) 10 final (in the following: DDPLE).
[90] Council of the European Union, 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) – Preparation of a general approach, 2012/0011 (COD) as at 11 June 2015, available at: http://data.consilium.europa.eu/doc/document/ST-9565-2015-INIT/en/pdf%20(in the following: GDPR in its version of 11 June 2015).
[91] Council of the European Union, 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 – Revised Version, 2012/0010 (COD) as at 29 June 2015, available at: http://statewatch.org/news/2015/jul/eu-council-dp-dir-leas-10335-15.pdf%20(in the following: DDPLE in its version of 29 June 2015); Council of the European Union, 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 – Chapters I, II and V modified, 2012/0010 (COD) as at 24 June 2015, available at: http://www.statewatch.org/news/2015/jul/eu-council-dp-dir-leas-chapI-II-V-10133-15.pdf%20(in the following: DDPLE in its version of 24 June 2015).

standards that data must be **adequate, relevant and not excessive** in relation to the original purpose(s) of processing, **accurate, kept up to date** and in a form which allows the identification of the data subject and kept **no longer than is necessary** in light of the purposes for which the data are processed.[92] These standards vary only slightly between the instruments. Framework Decision 2008/977/JHA, for instance, refers in a less strict wording to the obligation to process only accurate data and keep them up to date.[93] Yet, Article 4 of DDPLE, which will replace this decision, entails a stronger wording, very closely resembling the wording mentioned above. Observably, there are differences between the version of the European Parliament, preferring a stricter wording and more detailed quality criteria, and the Council's position leaving a greater leeway to Member States.[94] Considering these differences in an LE context where the quality of data plays an essential role in investigations and in situations where data are exchanged with other authorities, having data of a high quality stored in LE files, serves the interests of both the data subject as well as LE.

Clearly, one of the core quality standards is the **purpose limitation principle**, meaning that data should not be further processed in a way that is incompatible with the purpose initiating the collection of this data.[95] The principle should exclude processing for unknown purposes and the possibility to subsequently alter the initial purpose. While the initial purpose must be clearly defined and legitimate before processing, derogations from this principle are possible, but must be expressly laid down in a legal basis. The existing EU LE instruments allow for processing for other purposes in restricted cases. Further processing for a different purpose is, for instance, permitted in Framework Decision 2008/977/JHA so far as it is not incompatible with the purposes for which the data were collected, has a legal basis and is necessary and proportionate to that other purpose.[96] In addition, further processing for LE related purposes, such as prevention, investigation, detection or prosecution of criminal offences may be allowed as well.[97] Although, in this case, the further processing needs to stay within the boundaries of necessity and proportionality.[98] If data are transmitted to another Member State, processing for other purposes is additionally allowed, if the transmitting Member State consents to this processing.[99] This clearly constitutes a far reaching derogation from the purpose limitation principle creating an exclusive decision right for an LE authority on data processing, disconnecting the data from their original purpose of collection.[100]

It is evident that the purpose principle is equally included in the DDPLE. Article 4 (1) (b) and (c), recitals (18) and (20) DDPLE refer to it, while Article 7 DDPLE specifies lawful purposes for which processing according to the DDPLE is allowed. Far reaching derogations, similar to the ones mentioned in Framework Decision 2008/977/JHA were recently

[92] Compare: Article 6 of Directive 95/45/EC, Article 4 of Regulation 45/2001, Articles 3 (1) and 4 (1) of Framework Decision 2008/977/JHA, Article 4 of DDPLE in its version of 29 June 2015, Article 5 of GDPR in its version of 11 June 2015.
[93] Article 4 (1) of Framework Decision 2008/977/JHA.
[94] Compare Article 4 of the European Parliament legislative resolution of 12 March 2014 on the 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, available at: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2014-0219+0+DOC+XML+V0//EN (in the following: DDPLE in its version of 12 March 2014); Article 4 of DDPLE in its version of 29 June 2015.
[95] Article 6 (1) (b) of Directive 95/46/EC; Article 3 (1) of Framework Decision 2008/977/JHA and Article 4 (1) (b) of Regulation 45/2001.
[96] Article 3 (2) of Framework Decision 2008/977/JHA.
[97] Article 11 of Framework Decision 2008/977/JHA.
[98] Articles 11, 3 (2) of Framework Decision 2008/977/JHA.
[99] Article 11 (d) of Framework Decision 2008/977/JHA.
[100] Critical: de Busser, pp. 103-105.

introduced by the Council in June 2015, in particular in Article 4 (2) DDPLE including a section where, "further processing by the same controller for another purpose shall be permitted in so far as: (a) it is (…) compatible with the purposes for which the personal data was collected; and (b) the controller is authorised to process such personal data for such purpose in accordance with the applicable legal provisions; and (c) processing is necessary and proportionate to that other purpose."[101] Article 4a DDLPE which in its form was introduced by the Parliament in March 2014, included restrictions on data initially processed for other purposes, was deleted by the Council in its 2015 version.[102] However, it is clear from both versions that the purpose limitation principle must also apply in the LE sector and that restrictions must reflect necessity and proportionality aspects.

The GDPR mentions the purpose limitation principle in its Article 5 (1) (b) requiring that data can be "collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes". Article 5 (1) (c) adds that data must further be "adequate, relevant and not excessive in relation to the purposes for which they are processed".[103] The purpose limitation principle is further specified in the subsequent articles, in particular in Article 6 specifying the conditions for a lawful processing. Such as with the DDPLE, the Council recently introduced a new Article 6 (3a) and (4) GDPR weakening this principle considerably by permitting further processing "by the same controller for incompatible purposes on grounds of legitimate interests of that controller or a third party (…), if these interests override the interests of the data subject".[104] However, whether this provision, as well as the similar provision in the DDPLE will find their way into the final version of the GDPR after the trilogue meetings is rather doubtful.

2.2.2. Rules for the Processing of Sensitive Data

In addition to quality standards, EU data protection legislation – independent of the policy – entails a general consensus on the protection of specific kinds of data which reveal racial or ethnic origin, political opinions, trade-union membership, religious or philosophical beliefs or data concerning health or sex life.[105] While these categories can be considered as broadly accepted, more recent data protection instruments show the intention to extend this specific protection to individual categories, including genetic data and data concerning criminal convictions or related security measures data.[106] In particular the latter category is subject to discussion.[107]

Usually, there is a general prohibition to process these special categories of data.[108] Derogations exist, but depend on the respective instrument. However, some general observations can be made. When comparing the different instruments, a tendency is to be observed to increase the level of transparency. While Directive 95/46/EC left a wide margin of discretion to the Member States, the GDPR describes the restrictions to the rule in more detail.[109] The same tendency is visible with regard to the development of LE data protection

[101] Article 4 (2) of DDPLE in its version of 29 June 2015.
[102] Article 4a of DDPLE in its version of 12 March 2014.
[103] Article 5 (1) (c) of GDPR in its version of 11 June 2015.
[104] Article 6 (4) of GDPR in its version of 11 June 2015; see also recital (40) of GDPR in its version of 11 June 2015.
[105] Article 8 (1) of Directive 95/46/EC; Article 9 (1) of GDPR and Article 9 of GDPR in its version of 11 June 2015; Article 6 of Framework Decision 2008/977/JHA; Article 8 (1) of DDPLE in its version of 29 June 2015.
[106] Article 9 (1) of GDPR and GDPR in its version of 11 June 2015; Article 8 (1) of DDPLE and DDPLE in its version of 29 June 2015.
[107] Compare Disagreement between Council decision and Commission proposal on inclusion of data concerning criminal convictions or related security measures: Article 8 of GDPR vs. Article 9a of GDPR in its version of 11 June 2015.
[108] Article 8 (1) of Directive 95/46/EC; Article 9 (1) of GDPR and GDPR in its version of 11 June 2015; Article 6 of Framework Decision 2008/977/JHA; Article 8 (1) of DDPLE in its version of 29 June 2015.
[109] Compare Article 8 (5) of Directive 95/46/EC.

rules. Framework Decision 2008/977/JHA generally permits processing of the special categories of data only when it is strictly necessary and if adequate safeguards in national law exist[110]. In contrast, the DDPLE refers to several specific exceptions with precisely defined purposes.[111] These exceptions must further comply with the principle of proportionality and must be necessary to reach a defined aim or a specific protected value.[112] This test is particularly important in the LE sector, due to the potential adverse effects data processing of such categories may have in an LE context.[113]

2.2.3. Independent Supervision

The protection of individual data protection rights is of particular importance in the framework of third state LE transfer. Only recently, in its data retention judgement, the Court emphasized the importance of independent supervision, which is difficult to guarantee, if data leaves the EU and are stored in countries with a different legal system, possibly not capable of guaranteeing similar protection mechanisms for individuals.[114] Not only other supervisory rules are the reason for special protection requirements in this context, it is also problematic to limit the further use of the transferred data, once they leave EU territory as well as to guarantee effective remedies, if, data are conceivably misused in third states. While the transfer to third states is already very difficult in an economic related context, LE connected transfer is even more problematic. Moreover, there are situations, in which both contexts mix, making it difficult to determine which rules actually apply. A recent example is the transfer of Facebook data, subject to the case *Schrems v. Data Protection Commissioner*, in which the Court was faced with the question, whether the economically related safe harbor framework enabling the transfer of the data to the US and, in this way, incidentally the subsequent access of US LE and secret service authorities to these data, violates EU fundamental rights.[115]

Independent supervision of data processing of personal data is therefore regarded as a crucial aspect of protection, whose importance was recently underscored by three CJEU cases, mentioned above.[116] The CJEU developed comprehensive criteria for the independency principle considering even the mere risk of influence on data protection authorities as a violation.[117] The development of criteria for this principle became necessary, because the existing instruments, such as Directive 95/46/EC and Framework Decision 2008/977/JHA merely state that the supervisory authority shall act with complete independence without stipulating detailed criteria for this principle. The new GDPR as well as the DDPLE specify this aspect by designating an entire article to the criteria for independent supervision.[118] Examples are that members of supervisory authorities must remain free from external influence, that supervisory authorities are sufficiently equipped with human, technical and financial resources, premises and infrastructure as well as with a separate financial budget.

[110] Article 6 of Framework Decision 2008/977/JHA.
[111] Article 8 (2) of DDPLE; Amendment 69 on Article 8 (2) of DDPLE in its version of 12 March 2014; Article 8 (2) of DDPLE in its version of 29 June 2015.
[112] Article 9 (2) of GDPR and GDPR in its version of 11 June 2015; Article 8 (2) of DDPLE; Amendment 69 on Article 8 (2) of DDPLE in its version of 12 March 2014; Article 8 (2) of DDPLE in its version of 29 June 2015.
[113] Amendment 69 on Article 8 (2) of DDPLE in its version of 12 March 2014; Article 8 (2) of DDPLE in its version of 29 June 2015.
[114] CJEU, C-293/12 and C-594/12 *Digital Rights Ireland*, para 68.
[115] CJEU, C-362/14 *Schrems*; compare also: Boehm, Legal opinion on the adequacy of the safe harbor decision.
[116] Article 28 (1) of Directive 95/46/EC, Article 47 (1) of GDPR, Article 25 (1) of Framework Decision 2008/977/JHA, Article 40 (1) of DDPLE; Recital 62 of Directive 95/46/EC, Recital 92 of GDPR, Recital 33 of Framework Decision 2008/977/JHA, Recital 51 of DDPLE; cases see above, section 2.1.2.2
[117] Cases see above, section 2.1.2.2.
[118] Article 28 (1) of Directive 95/46/EC, Article 47 GDPR in its version of 11 June 2015, Article 25 (1) of Framework Decision 2008/977/JHA and Article 40 of DDPLE in its version of 29 June 2015; compare also former versions of this article, which are more exhaustive.

To improve cooperation between the different national data protection authorities, the GDPR establishes new tools such as the consistency mechanism and an European Data Protection Board (EDPB), which will replace the current Article 29 Working Party on the Protection of Individuals.[119] While the Working Party did not cover situations arising in the LE sector, the new DDPLE is going to incorporate the EDPB into the supervision of data processing in this field.[120] Article 49 DDPLE establishes an advisory status for the EDPB on questions regarding data protection in LE matters on request of the Commission or on its own initiative, including the issue (and review) of guidelines, recommendations and best practices in order to contribute to the consistent application of the DDPLE. The EDPB should be also involved in the assessment of the level of protection in third states or international organizations.

In addition to the supervisory authorities, controllers and processors shall (or may in the Council's version) establish the position of a data protection officer monitoring internal data processing within entities.[121] This position should also exist in LE organizations.[122] At EU level, LE bodies, such as Europol or Eurojust have established this position since years within their institutions.[123]

2.2.4. Transfer to Third States

The most important procedure to transfer data to third countries was established by Directive 95/46/EC with the **adequacy mechanism**. Articles 25 (1) and (2) of Directive 95/46/EC allow data transfer to a third state, if the third state ensures an adequate level of protection. The level of adequacy is assessed by the Commission in light of all the circumstances surrounding a data transfer. Particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation, 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 rules and security measures which are complied with in the country.[124] The Article 29 Working Party has summarized in various documents the core principles with which third countries must comply with to assure an adequate level of protection. They refer to the respecting of the purpose limitation principle, the data quality and proportionality principle, the transparency principle, the security principle, the rights of access, rectification and opposition and restrictions on onward transfers.[125] These substantial guarantees should be complemented by procedural mechanisms such as sanctions for data processors in case of non-compliance with data protection rules, a right to redress for individuals or the establishment of supervisory authorities with monitoring and investigation functions.[126] Based on these principles, the Commission has adopted several adequacy decisions for entire countries, such as Argentina, Canada, Israel or Switzerland.[127] A special mechanism applies with regard to data transfers to the US. The so called **safe harbor regime** establishes a self-

[119] Articles 54a et seq. and 64, 65 of GDPR in its version of 11 June 2015.
[120] Article 49 of DDPLE in its version of 29 June 2015.
[121] Articles 35 and 36 GDPR in its version of 11 June 2015 and Article 30 of DDPLE in its version of 29 June 2015.
[122] Article 30 of DDPLE in its version of 29 June 2015.
[123] Article 28 of Council Decision 2009/371/JHA of 6 April 2009 establishing the European Police Office (Europol), OJ L 121, 15.5.2009, p. 37 – 66 (in the following: Europol Decision 2009/371/JHA); Article 17 of Council Decision 2002/187/JHA of 28 February 2002 setting up Eurojust with a view to reinforcing the fight against serious crime, OJ L 63, 6.3.2002, p. 1 – 13.
[124] Article 25 (2) of Directive 95/46/EC.
[125] Document adopted by the Article 29 Working Party, WP 12 of 24 July 1998 on the transfers of personal data to third countries: applying Articles 25 and 26 of the EU data protection directive (in the following: WP 12 of 24 July 1998) combined the working papers WP 4 of 26 June 1997, WP 7 of 14 January 1998, WP 9 of 22 April 1998 and WP 114 of 25 November 2005.
[126] WP 12 of 24 July 1998, p. 5.
[127] Compare: http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm.

certifying system permitting participating US companies to transfer data from the EU to the US. In a decision from July 2000 the Commission accepted this mechanism as constituting an adequate protection for individuals.[128] The validity of this decision is subject to aforementioned case *Schrems v. Data Protection Commissioner* and is therefore analyzed in more detail in the next section.[129] In absence of an adequacy decision, transfer of data to third states is possible in particular cases under the conditions of Article 26 of Directive 95/46/EC.

Transfer of data in a purely LE context partly derogates from the Directive's provisions. Institutions such as **Europol or Eurojust** have developed their own transfer system under the former third pillar framework by being allowed to conclude exchange agreements with various third states, including with those not providing for an adequate level of protection within the framework of Directive 95/46/EC.[130] However, Europol, for instance, must in this case assess that the third state ensures an adequate level of protection with regard to the transfer.[131] The criteria leading to this specific adequacy finding should in principle correspond to those of Directive 95/46/EC, although this is not particularly stipulated in Europol's legal basis, but can be derived from a common understanding of terms in EU law. According to the proposed Europol Regulation, the possibility to conclude data exchange agreements individually will vanish and be replaced by a provision permitting transfer in case of an existing adequacy decision of the Commission, an international agreement concluded between the EU and a third country or international organization or in specific cases mentioned in Article 31 (2) of this proposal.[132] The adequacy standard of Directive 95/46/EC (or of the succeeding GDPR) will therefore also become the standard for transfer with regard to LE data.

The transfer procedure provided for in LE **Framework Decision 2008/977/JHA** is not as detailed as the one in Directive 95/46/EC, although the criteria for adequacy stipulated in Article 13 (4) principally mirror the Directive's criteria.[133] Article 13 (1) Framework Decision 2008/977/JHA specifies the conditions under which personal data may be transferred to third states or international bodies. Basically, data can be transferred, if they are necessary for LE related cases (mentioned are prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties) and with the consent of the Member State where the data originated from, to LE bodies in third states, if the third state or international body concerned ensures an adequate level of protection for the intended data processing. As the rules of Framework Decision 2008/977/JHA are limited to cross-border data exchange and do not apply to domestic LE data processing, relatively broad exceptions considering the national interests of Member States exist. Derogations from the aforementioned guarantees apply in cases in which (a) the national law of the Member State transferring the data provides so for because of: (i) legitimate specific interests of the data subject or (ii) legitimate prevailing interests, especially important public interests or (b) the third state or receiving international body provides safeguards which are deemed

[128] Commission Decision 2000/520/EC of 26 July 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, OJ L 215, 25.08.2000, p.7 – 47 (in the following: Safe Harbor decision).
[129] Compare section 2.2.5.
[130] For Europol compare: Council Decision 2009/935/JHA of 30 November 2009 determining the list of third States and organisations with which Europol shall conclude agreements, OJ L 325, 11.12.2009, p. 12–13; Council Decision 2009/934/JHA of 30 November 2009 adopting the implementing rules governing Europol's relations with partners, including the exchange of personal data and classified information, OJ L 325, 11.12.2009, p. 6 – 11.
[131] Article 23 (6) (b) of Europol Decision 2009/371/JHA.
[132] Article 31 of the Proposal for a Regulation of the European Parliament and of the Council on the European Union Agency for Law Enforcement Cooperation and Training (Europol) and repealing Decisions 2009/371/JHA and 2005/681/JHA, COM(2013) 173 final (in the following: Europol Regulation).
[133] Compare Article 13 (4) of Framework Decision 2008/977/JHA.

adequate by the Member State concerned according to its national law.[134] In addition to the transfer to third states, data can also be transmitted to private parties.[135]

Transfer to third states in the **GDPR** is regulated in a similar way as in Directive 95/46/EC, although in a more comprehensive way. Its Chapter V dedicates detailed rules to this important aspect. In particular Article 41 GDPR contains detailed rules on data transfer to third states. It is worth saying in advance that, although with regard to other proposed provisions in the GDPR there are quite remarkable differences to be observed between the proposals of the Commission, the Parliament and the Council, this article seem to be less disputed. The adequacy mechanism of Directive 95/46/EC is maintained, although stipulated in greater detail by clarifying, amongst others, that an adequacy decision can relate to a country, a territory or a specified sector within a third country or an international organization.[136] The criteria according to which adequacy should be determined are extended compared to Directive 95/46/EC and include important aspects such as the rule of law, respect for human rights and fundamental freedoms, relevant legislations, including rules for onward transfer of personal data to another third country or international organization, the existence of effective and enforceable data subject rights and effective administrative and judicial redress for data subjects as well as the existence and effective functioning of independent supervisory authorities including adequate sanctioning powers.[137] International commitments, in particular in relation to data protection, of the third country or the international organization should also be taken into account. While the Parliament particularly mentions legislation concerning public security, defence, national security and criminal law, the wording of a Council is less detailed, but does not exclude that LE legislation is considered when deciding on the level of adequacy.

As the level of protection may change over the years, both the Parliament's as well as the Council's position demand a continued monitoring of the legal situation in third states through the Commission and intend to establish the possibility to revoke an adequacy decision once made, if the adequate level is no longer ensured anymore.[138] While the details of this process may vary slightly, the common denominator between these positions will most likely be a periodical review of the adequacy decisions including a possibility to revoke the decision, similar to the proposals made by the EDPS.[139] Existing adequacy decisions shall remain in force until they are amended, replaced or repealed. The Parliament additionally proposes to obligatory replace the decisions on basis of Directive 95/46/EC after a period of 5 years.[140] In absence of an adequacy decision or in case it is decided that an adequate level cannot be assured by the third party, the latter must guarantee appropriate safeguards covering onward transfers laid down in a legally binding and enforceable instrument in form of approved binding corporate rules (Article 43 GDPR), standard data protection clauses or contractual clauses (Parliament), respectively an approved code of conduct together with binding and enforceable commitments (Council).[141]

[134] Article 13 (3) of Framework Decision 2008/977/JHA.
[135] Article 14 of Framework Decision 2008/977/JHA, critical on this provision: EDPS, Third opinion on Framework Decision 2008/977/JHA, OJ 2007 C 139, 23.6.2007, paras 34-36.
[136] Article 41 (1) of GDPR in its version of 11 June 2015.
[137] Article 41 (2) of GDPR in its version of 11 June 2015.
[138] Article 41 (2a) to (5a) of GDPR in its version of 11 June 2015; Article 41 (3) of European Parliament legislative resolution of 12 March 2014 on the 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), available at: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2014-0212+0+DOC+XML+V0//EN (in the following: GDPR in its version of 12 March 2014).
[139] Compare: EDPS, Annex to Opinion 3/2015, available at: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2015/15-07-27_GDPR_Recommendations_Annex_EN.pdf.
[140] Article 41 (8) of GDPR in its version of 12 March 2014.
[141] Article 42 of GDPR in its version of 11 June 2015.

Additionally, approved certification mechanisms or the possibility of a valid "European Data Protection Seal" (proposal of the Parliament) should be accepted as a further safeguard to transfer data to third states.[142] The Council also wants to accept a legally binding and enforceable instrument between public bodies and authorities as an appropriate safeguard.[143] Some safeguards should be subjected to prior authorization by the competent supervisory authority, amongst other, contractual clauses or provisions of administrative arrangements between public authorities and bodies.[144] The latter category was equally introduced by the Council in June 2015.

In addition to these rules, the Parliament and the EDPS propose to introduce a provision regulating transfers or disclosures not authorized by EU or Member States law. A new Article 43a GDPR includes rules on third state access to data stored within the EU. It should hinder third countries to acquire the disclosure of data via judgments or administrative decisions from controllers or processors based in the EU. An EU controller or processor receiving such an order should notify the competent supervisory authority, which can authorize the respective transfer or disclosure in case it complies with necessity requirements and it is legally required to according to the rules of the GDPR (Article 44).[145] If relevant, the supervisory authority must apply the consistency mechanism. According to the proposal of the Parliament, the supervisory authority should also inform the individual concerned of the request and, if possible, the decision of the supervisory authority.[146]

Rules on transfer of LE data to third states within the **DDPLE** are currently being discussed between the Member States. Recent documents on chapter V regulating this issue as well as the differences between the positions of the Councils and the EP, however, indicate that a compromise on these rules seems to be far from being adopted.[147] Consequently, the following section can merely reflect an intermediary state of this discussion.

Within the framework of LE data transfer to a third state, the adequacy of the level of protection equally plays a crucial role for the rights of individuals concerned. Transferring LE data to third states considerably enlarges the number of authorities accessing and possibly further transferring the data. Additionally, data are transmitted to a complete different jurisdiction leading to the consequence that the enforcement of individual rights and remedies becomes increasingly difficult.[148] Data protection rules of third states in the LE sector are therefore of particular importance. To provide adequate protection in this specific field, data protection rules in third states must therefore equally correspond to the level of protection provided for LE related data within the EU.

So far, the level of protection in third states in this specific field was not yet a particular subject for considering the level of adequacy in existing decisions of Directive 95/46/EC, which is due to the fact that the latter does not apply to LE related matters. Article 41 GDPR regulating the adequacy mechanism in its latest version mentions more criteria to be considered when deciding on the level of protection in third states then Directive 95/46/EC, but does not contain a special reference to LE rules of the third country either. This reference was initially included in the Commission's as well as in the Parliament's version of the GDPR.[149] In the latest version of the Council, it was decided to erase the particular

[142] Articles 42 (2) (aa) of GDPR in its version of 12 March 2014 and 42 (2) (e) of GDPR in its version of 11 June 2015.
[143] Article 42 (2) (oa) of GDPR in its version of 11 June 2015.
[144] Article 42 (2a) (d) of GDPR in its version of 11 June 2015.
[145] Article 43a of GDPR in its version of 12 March 2014; EDPS, Annex to Opinion 3/2015.
[146] Article 43a (4) of GDPR in its version of 12 March 2014.
[147] Compare DDPLE in its version of 29 June 2015 and the respective Chapter V in DDPLE in its version of 24 June 2015.
[148] Compare CJEU, C-293/12 and C-594/12 *Digital Rights Ireland,* para. 68 (with regard to supervision).
[149] Article 41 (2) (a) of GDPR in its version of 12 March 2014.

section mentioning the rules regarding the fields of public security, defence, national security and criminal law.[150] Instead there is a more general reference to general and sectoral data protection rules, which could naturally embrace LE data protection rules. The reason for the detailed mentioning of the adequacy mechanism in the GDPR in this study is that Article 34 (1) DDPLE refers to the conditions for transfer and includes in both the Commission's as well as the Council's version a reference to the adequacy decision taken in the framework of Article 41 GDPR. Both proposals provide for a transfer to a third country, if an adequacy decision within the GDPR has been taken. If, however, this reference is made, the adequacy criteria in the GDPR should obviously include the assessment of the third country's sectorial LE rules as proposed by the EP as well as a clarification that existing adequacy decisions cannot serve as justification to transfer data, as such decisions did not include an assessment of the LE sector.

In absence to an adequacy decision within the GDPR framework, the Commission can also assess the adequacy of a transfer to third states, a specific sector in a third state, a territory or an international organization according to specific LE criteria mentioned in Article 34 (2) DDPLE. These criteria explicitly refer to the general standards of the respect to the rule of law, respect for human rights and fundamental freedoms, the existence of effective and enforceable data protection rights as well as effective administrative and judicial redress possibilities and additionally include LE related specifics, such as the data protection rules concerning public security, defence, national security, criminal law, security measures including rules for onward transfer of data to other third states or organizations.[151] Further, they refer to the existence and effective functioning of independent supervisory authorities with adequate sanctioning powers as well as international commitments or other obligations the third country is subject to.[152] The Commission is said to monitor these decisions and can revoke them, if it considers the adequate level of protection is not ensured anymore.[153]

While the consequences for such a revoking decision are still disputed, Article 35 and 36 DDPLE provide for further transfer possibilities in absence of an adequacy decision.[154] According to Article 35 DDPLE, appropriate safeguards laid down in a legally binding and enforceable instrument or an assessment of the controller coming to the conclusion that appropriate safeguards exist in a specific case should be equivalent to an adequacy decision of the Commission. As the provision is still in the drafting process, the relationship to the criteria mentioned in Article 34 (2) DDPLE is not yet clear, but from the point of coherency, it would make no sense to apply different criteria in this context. Otherwise, in regards to the fact that most transfers of LE data to third countries happen in absence of an adequacy decision, different criteria would lower the transfer standard considerably. Derogations from the transfer in specific situations are included in Article 36 DDPLE, relating, amongst other, to situations in which the transfer is necessary to prevent an immediate and serious threat to public security or in individual cases for LE purposes. Paragraph (2) of Article 36 DDPLE provides for a proportionality clause stipulating that data should not be transferred, if in an individual case, the interests of the data subject override the public interests mentioned in the first paragraph. If data are updated, rectified or erased after they have been transferred, the Parliament plans to introduce a notification requirement for the controller transferring the data to the third state.

[150] Compare Article 41 (2) (a) of GDPR in its version of 11 June 2015.
[151] Article 34 (2) (a) of DDPLE in its version of 29 June 2015.
[152] Article 34 (2) (b) and (c) of DDPLE in its version of 29 June 2015.
[153] Article 34 (4a) and (5) of DDPLE in its version of 29 June 2015.
[154] Compare the different versions of Article 34 (6) of DDPLE in its version of 29 June 2015 (including the comments of the different Member States) and of DDPLE in its version of 12 March 2014.

2.2.5. Exchange in the Framework of Safe Harbor

As the scope of this study refers to LE data protection legislation within the EU and the US, it is important to briefly mention the data exchange in the framework of Safe Harbor (from here on SH), which is currently subject to the *Schrems* case mentioned above.[155] In absence of a general adequacy finding for the US, another possibility had to be established to transfer data to the US resulting in the SH decision in 2000, which basically created a self-certifying mechanism for US companies transferring data to the EU.[156] The SH decision derogates from the usual formal requirements of adequacy decisions by accepting "principles" and "FAQs" issued by the US Department of Commerce and annexed to the SH decision as guarantees for an adequate level of protection.[157] The signing of the principles in the US allow US companies to transfer data from the EU to the US. Since years, the functioning of this mechanism has been subject to harsh criticism, even from the Commission itself. In 2013, after it was revealed that US intelligence agencies accessed mass amounts of data transferred to the US by SH companies, the Commission issued a list of 13 recommendations, which should improve the existing SH regime and started negotiations on a new SH framework.[158] Until now, the discussions with the US are ongoing. In consequence, data transfers based on the SH decision are still continuing. The shortcomings and differences of the EU data protection framework to the existing SH mechanism shall be briefly mentioned to allow for a complete picture of the current data exchange between the EU and the US.[159] These shortcomings were recently confirmed in the opinion of Advocate General Bot in the *Schrems* case.[160]

A remarkable weakness of the existing SH regime relates to its **scope of application**, which enables a wide ranging use of data outside the sphere of protection of SH. The application of the self-certified system is limited to certified organizations, meaning that all government authorities and all non-certified organizations in the US are not part of the SH system. However, transfers to non-certified organization happen regularly and are even covered by the scope of SH, as the SH principles are subject to US interpretation.[161] **Any law, government regulation and case law can override the self-certification mechanism and national security, public interest and law enforcement requirements make the SH non-applicable**, even though they are not specified in a law, government regulation or case law.[162] Annex IV of the SH decision additionally states that not only a duty to provide data, but also a "special authorization", for instance, to share data, overrides the SH principles. Consequently, the scope of application of the SH principles is limited to cases in which no other specific regulation within the US legal system applies. As US laws and the US constitution do not grant privacy protection for non-US persons, protection for EU citizens is therefore very limited outside, and even within, the framework of SH. [163]

[155] See above at section 2.1.3.5.
[156] Safe Harbor Decision, OJ L 215, 25.08.2000, p.7 – 47.
[157] All adequacy decisions are available via this link: http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm.
[158] Communication from the Commission to the European Parliament and the Council on the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU, COM/2013/0847, pp. 18 and 19 (in the following: Communication on Functioning of Safe Harbor).
[159] The section bases on the findings of a legal opinion prepared by the author of this study: Boehm, Legal opinion on the adequacy of the safe harbor decision, available at: http://www.europe-v-facebook.org/CJEU_boehm.pdf.
[160] CJEU, C-362/14 *Schrems*, opinion of 23rd of September, available at: http://curia.europa.eu/juris/document/document.jsf?text=&docid=168421&pageIndex=0&doclang=en&mode=req&dir=&occ=first&part=1&cid=518391.
[161] Sixth paragraph of Annex 1 to the Safe Harbor Decision.
[162] Fourth paragraph of Annex 1 to the Safe Harbor Decision.
[163] For the US privacy framework, compare: Bowden/Bigo, p. 19; Bignami pp. 10 et seq.

With regard to **substantive law guarantees**, in particular the data quality principles mentioned in the SH decision, important minimum standards (fairness, lawfulness, adequacy, explicit purpose limitation) are not applied at all or applied in a less stringent way. Whereby at first view, the SH decision seem to contain most of the important principles of EU data protection law, a closer analysis reveals several weaknesses. Important EU data protection principles, such as "fairness" and "lawfulness" and "adequacy" are missing. In particular the lack of the latter element is problematic, as in its absence there is no starting-point for conducting the proportionality test which is crucial in European data protection legislation.[164]

While EU data protection law follows the approach that data processing is generally prohibited, unless it does not comply with an exemption allowing for processing, the SH decision establishes the opposite. Processing depends on the application of the **notice and choice** principle, which turns the general prohibition to process personal data into a **general permission for processing**.[165] Further, the applicability of the choice principle (opt-out) is limited to only two situations, which are "usage for another purpose" or "disclosure to a third party".[166] Both criteria are also the only limitations entailed in Safe Harbor on **onward transfer** to third parties. There are some rules on transfer to data processors (called agents), but all other transfers are not regulated.[167] In addition, as mentioned above, both principles can be easily overridden by US law, for instance by a provision requiring to transfer data to intelligence agencies such as the FISA provisions mentioned beneath in section 3.4. The notice principle, meaning informing the data subject about the processing, is formulated in a way that leaves considerable leeway to companies when applying this principle.[168] In practice, companies transferring data in the SH framework formulate a broad processing purpose at the moment when the data are first collected, with the consequence that in case the data are transferred to the US, no further informing the data subject needs to take place.[169] This can easily lead to situations in which individuals "may not be made aware by […] companies that their data may be subject to access" by third parties.[170]

Data protection **rights of individuals such as access, correction, rectification and deletion** are stated in the SH decision, but lack further specification.[171] The only right which is described in more detail is the right of access. FAQ 8 of Annex II dedicates a whole paragraph to this issue, mainly stipulating various exceptions and limitations to this right. Examples in practice show the difficulties individuals face when requesting access to data transferred to the US within the SH framework.[172] The other mentioned rights to deletion, correction and amendment are limited to data that is "inaccurate", thereby restricting the possibility of the individual to remedy data that may be illegally processed, but not inaccurate.[173]

A final, but an important point of criticism concerns the theoretical and practical **enforcement of remedies**, sanctions and **notification** duties as well as the

[164] Compare Article 29 Data Protection Working Party, Opinion 01/2014, available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp211_en.pdf.
[165] Compare the provisions on notice and choice, Annex 1 to the Safe Harbor Decision.
[166] Compare the provision on choice, Annex 1 to the Safe Harbor Decision.
[167] Compare the provisions on onward transfer, Annex 1 to the Safe Harbor Decision.
[168] Compare for a detailed analysis: Boehm, Legal opinion on the adequacy of the safe harbor decision, pp. 11-14.
[169] For broad processing purposes, compare https://de-de.facebook.com/about/privacy/%20 and https://www.facebook.com/legal/terms.
[170] Compare Communication on Functioning of Safe Harbor, pp. 16 et seq., in particular para 7.3.
[171] Compare the provisions on access, Annex 1 and FAQ 8, Annex 2 to the Safe Harbor Decision.
[172] CJEU, C-362/14 *Schrems*.
[173] Compare the provisions on access, Annex 1 to the Safe Harbor Decision.

establishment of **independent supervisory bodies** within the SH framework. The SH decision does not provide for any independent cause of action due when the right to data protection is violated. It refers to the existing civil law claims in US law and establishes an Alternative Dispute Resolution (ADR) mechanism, including some limited powers of the Federal Trade Commission (FTC).[174] The latter's legal authority is restricted to remedy possible violations of section 5 of the FTC Act concerning unfair and deceptive acts or practices in commerce. Other violations of the SH principles, including, for instance, the accessing of SH data by intelligence agencies, are not within its authority. The same applies in regards to ADR mechanisms which are further considered as being neither effective, nor provide independent supervision of data processing activities.[175] Additionally, ADR mechanisms "lack appropriate means to remedy cases of failure to comply with the [SH] principles" and they do not possess the power to actively investigate possible data protection violations or carry out any form of external control.[176] Moreover, they are chosen by the company allegedly violating the law. Oversight of the SH principles is therefore shifted to private organizations who do not have investigative powers and cannot be regarded as independent. In addition, it is worth noting that the initial self-certification is carried out by the companies themselves, by sending a letter to the Department of Commerce with basic information about the organization.[177] The Commission therefore states that there is "no full evaluation of the actual practice in self-certified companies" and demands "an active follow up by the Department of Commerce on effective incorporation of the Safe Harbor principles […]."[178] The oversight mechanism, as well as the remedy enforcement system of the SH decision therefore lacks important data protection guarantees.

In summary, it is widely recognized and visible from the above mentioned that there are considerable shortcomings when it comes to the protection and the enforcement of individual rights in the existing SH framework. The SH decision in its current version allows for wide-ranging derogations from EU data protection principles violating core data protection principles, including procedural as well as substantive guarantees, such as purpose limitation, independent supervision effective remedies, limitations on onward transfer, redress and access rights. The Commission initiated negotiations in 2013 to remedy part of these deficiencies, but, so far, without a tangible solution, in particular the question of the accessing of data transferred in the SH framework by intelligence services is not yet resolved.

2.2.6. Time-limits

Time limits play an essential role in safeguarding the data subject's privacy interests. It is broadly accepted that data must be kept in a manner which permits identification of data subjects, for no longer than necessary, for the purposes for which the data were collected or for which they are further processed.[179] In specific cases, stipulated for instance in Article 17 GDPR, the data subject has the right to obtain the erasure of data from the controller. Reasons for erasure are, amongst others, if data are no longer necessary for the purpose for which they were collected or processed, if consent is withdrawn and there is no other legal ground for processing, the data subject objects to the processing (and there is no overriding legitimate reason for processing) or in the case that data have been

[174] Annex II, FAQ No 11 and Annex IV to the Safe Harbor Decision.
[175] Communication on Functioning of Safe Harbor, pp. 14-15, in particular para 6.1, footnote 46 in the communication.
[176] Communication on Functioning of Safe Harbor, p. 10, in particular para 5.
[177] Annex II, FAQ No 6 to the Safe Harbor Decision.
[178] Communication on Functioning of Safe Harbor, p. 8, in particular para 4.
[179] Article 6 (1) (e) of Directive 95/46/EC; Article 17 of GDPR in its version of 11 June 2015; Article 5 of Framework Decision 2008/977/JHA; Article 4 (e) of DDPLE in its version of 29 June 2015.

unlawfully processed. The deletion of data of children should be prioritised.[180] In some instruments, the general principle of erasure is further specified by implementing mechanisms and procedures to ensure that the time limits are observed in practice. Periodical review of the stored data to verify whether the need for storage still exists, are, for instance, included in Framework Decision 2008/977/JHA as well as in the Commission's GDPR proposal.[181] Moreover, Framework Decision 2008/977/JHA contains a possibility for the transmitting authority to indicate a time limit for the retention that must be respected by the receiving authority.[182] The wording of the succeeding provision in the DDPLE concerning the introduction of procedural rules on rectification, erasure and blocking is currently still being disputed.[183] Related to the procedural rules is the obligation to inform the data subject about the length of the retention period when the data are collected and/or at least, if access requests are made.[184] In addition, the GDPR provides for a documenting requirement including, *inter alia*, the duty to document the envisaged time limits for erasure of the different categories of data.[185]

2.2.7. Rights and Remedies of Individuals

Rights of individuals primarily include **information, access, rectification, erasure, blocking, objection and notification** rights. These rights are contained in LE as well as other data protection instruments.[186] Between the different policy areas the provisions on restrictions of these rights evidently vary, but in all cases they must be necessary and proportionate with due regard to the interest of the individual concerned.[187] Although this aspect is already evident from primary law, its mentioning in the LE sector is crucial, as the exercising of these rights is the pre-condition for corrective measures, remedies and possible sanctions.[188] Restrictions in the LE sector mainly concern the prevention of hindering ongoing investigations or prejudicing other LE related purposes, to protect public or national security or the rights and freedoms of others.[189]

The **information** of the data subject needs to be carried out independently of the fact whether data has been collected directly from the data subject or obtained by a third party. In the LE sector, it includes at least basic information about the controller, the purpose of the collection and the right to lodge a complaint to a supervisory authority.[190] In recent years the information obligations, also in the LE sector, have become more detailed. It is for instance proposed to inform additionally about the legal basis for processing, the data retention period, the existence of the right to request from the controller access to and rectification, erasure or restriction of processing, the recipients of the data, including third parties or states, whether profiling measures are used and security measures taken.[191]

[180] Article 17 (1a) of GDPR in its version of 11 June 2015.
[181] Article 5 of Framework Decision 2008/977/JHA and Article 17 (7) GDPR.
[182] Article 9 of Framework Decision 2008/977/JHA.
[183] Compare discussion about the introduction of a new Article 4a in the DDPLE in its version of 29 June 2015 (footnote 165).
[184] Articles 14 (1) (c) and 15 (1) (d) of GDPR in its version of 11 June 2015 and Article 12 (1) (d) of DDPLE in its version of 29 June 2015.
[185] Article 28 (2) (g) of GDPR in its version of 11 June 2015.
[186] Chapter III of DDPLE in its version of 29 June 2015; Chapter III of GDPR in its version of 11 June 2015; Articles 16-20 of Framework Decision 2008/977/JHA; Chapter II, section IV-VII and IX of Directive 95/46/EC.
[187] Compare, for instance, Article 11b of DDPLE in its version of 29 June 2015.
[188] CJEU, C-293/12 and C-594/12 *Digital Rights Ireland*, paras 54 et seq. and ECtHR case law, see above, sections 2.1.3.3. and 2.3.
[189] Article 17 of Framework Decision 2008/977/JHA.
[190] Articles 11 and 11a of DDPLE in its version of 29 June 2015.
[191] Article 11 of DDPLE in its version of 12 March 2014.

Closely linked to the right of information is the **access right** of the person concerned.[192] In an LE context, it includes, so far, at least a confirmation whether data have been processed or not, which data undergo processing, to whom the data have been made available to and a confirmation, if verifications have taken place.[193] Refusals or restrictions of the access right, including the reasons therefore, should be communicated to the persons concerned in writing.[194] The recent DDPLE proposal shows the tendency to extend the access right by aligning it with the provisions on access in other policy areas. Access requests shall then at least additionally include the purpose of processing, the recipients of the data, including third countries, information on the data retention period as well as on the rights to rectification, erasure, restriction or to lodge a complaint to a supervisory authority.[195]

The rights to obtain **rectification, erasure and blocking as well as the notification** of any of those actions to a third party to which the data have been transmitted are core principles in all policy areas in EU data protection law.[196] Framework Decision 2008/977/JHA includes these rights and additionally provides a time-limit where data must compulsorily be deleted upon its expiry.[197] Inaccurate data must be rectified or completed.[198] If rectification, erasure or blocking is refused, the refusal must be communicated in writing to the person concerned.[199] Discussions about the design of these rights within the DDPLE framework are still ongoing and seem to be rather diverse.[200]

Effective **remedies** against infringements of privacy and data protection rights, the **right to receive compensation and to lodge a complaint at a supervisory authority** are fundamental to the EU legal system and included in all legislative data protection instruments, regardless of the policy area concerned.[201] Remedies, compensation requests and complaints to supervisory authorities can be invoked by individuals, independent of their nationality or residency. While in existing legislation, compensation is only mentioned in context with claims against the controller, the GDPR and the DDPLE introduce a right to also receive compensation from the processor.[202] Moreover, judicial remedies can also be directed against decisions of supervisory authorities.[203] This right can be exercised by the individual or, according to recent proposals, in specific situations by organisations or associations acting on behalf of the individual concerned.[204]

2.2.8. Automated Decision and Profiling

Subjecting the individual to decisions basing solely on automated processing which produce a legal effect is usually prohibited in EU data protection law, including in the LE sector.[205]

[192] Article 12 (1) (a) of Directive 95/46/EC; Article 15 of GDPR in its version of 11 June 2015; Article 17 of Framework Decision 2008/977/JHA; Article 12 of DDPLE in its version of 29 June 2015.
[193] Article 17 of Framework Decision 2008/977/JHA.
[194] Article 17 (3) of Framework Decision 2008/977/JHA.
[195] Article 12 (1) of DDPLE in its version of 29 June 2015.
[196] Article 12 (b) and (c) of Directive 95/46/EC; Articles 16 to 17b of GDPR in its version of 11 June 2015; Article 4 of Framework Decision 2008/977/JHA; Article 15 of DDPLE in its version of 29 June 2015; Articles 15 and 16 of DDPLE in its version of 12 March 2014.
[197] Articles 4, 5, 8 and 18 of Framework Decision 2008/977/JHA.
[198] Article 4 (1) of Framework Decision 2008/977/JHA.
[199] Article 18 (1) of Framework Decision 2008/977/JHA.
[200] Compare discussion surrounding Article 15 of DDPLE in its version of 29 June 2015.
[201] Articles 22, 23 and 28 of Directive 95/46/EC; Articles 73, 75, and 77 of GDPR in its version of 11 June 2015; Articles 19, 20 and 25 of Framework Decision 2008/977/JHA; Articles 50, 52 and 54 of DDPLE in its version of 29 June 2015.
[202] Article 77 (1) of GDPR in its version of 11 June 2015 and Article 54 (1) of DDPLE in its version of 29 June 2015.
[203] Article 28 (3) of Directive 95/46/EC; Article 74 of GDPR in its version of 11 June 2015; Article 25 (2) (c) of Framework Decision 2008/977/JHA, Article 51 DDPLE in its version of 29 June 2015.
[204] Article 76 of GDPR in its version of 11 June 2015 and Article 50 of DDPLE in its version of 29 June 2015.
[205] Article 15 of Directive 95/46/EC; Article 20 of GDPR in its version of 11 June 2015; Article 7 of Framework Decision 2008/977/JHA; Article 9 of DDPLE in its version of 29 June 2015.

LE instruments usually add the need for legal effects to be of adverse nature.[206] However, the general prohibition to be subjected to automated decisions can be restricted by a law, which must, however, include appropriate safeguards.[207] Recent proposals, such as the GDPR and the DDPLE additionally include provisions on profiling, which is referred to as being a sub-element of automated decisions. Profiling is defined as "any form of automated processing of personal data consisting of using those data to evaluate personal aspects relating to a natural person, in particular to analyze and predict aspects concerning performance at work, economic situation, health, personal preferences, or interests, reliability or behaviour, location or movements."[208] Containing the most comprehensive rules on this aspect, the GDPR provides, for instance, for the right of the individual to obtain information on the existence of profiling and the logic involved, as well it requires impact assessment, if processing is to be based on profiling methods.[209] Although provisions on profiling within the DDPLE LE context are less detailed, the proposed provisions indicate an increased awareness for the dangers resulting from profiling methods used in LE data processing.

2.2.9. Security and Technical Protection

Another essential data protection principle refers to data security measures, which ensure the implementation of technical and organizational measures to protect the stored data from misuse, loss and unlawful access. Although there are differences in scope and with regard to the details of the security obligations, LE and all other EU data protection instruments include provisions on this aspect.[210] Over the years, legislation on this aspect has become more specific, in particular by referring to ideas such as privacy by design, which contributes to more sophisticated technical solutions.[211] Usually, a list of precautions which are to be implemented, such as equipment access control, data media control, user, transport and input control or data access control to prevent unauthorised access to data, are included in the provisions on security measures.[212] To incentivise the implementation of data security measures, the GDPR as well as the DDPLE provide for data breach notifications to supervisory authorities or the individuals concerned.[213]

2.3. Council of Europe

When determining the EU data protection framework in the LE sector, the guarantees of the Council of Europe, especially Article 8 ECHR and the respective ECtHR case law play an essential role. Other instruments, such as Convention No. 108 and Recommendation R (87) 15 complete the Convention's protection, but play a less important role in practice.[214]

The importance of Article 8 ECHR for data protection in LE must not be underestimated. As mentioned above in section 2.1.2.4., the CJEU did not deliver any judgements in data

[206] Article 7 of Framework Decision 2008/977/JHA; Article 9 of DDPLE in its version of 29 June 2015.
[207] Article 7 of Framework Decision 2008/977/JHA; Article 9 of DDPLE in its version of 29 June 2015.
[208] Article 4 (12a) of GDPR in its version of 11 June 2015 and Article 3 (12a) of DDPLE in its version of 29 June 2015.
[209] Articles 14 (1) (h) and 15 1 (h) of GDPR in its version of 11 June 2015; Article 33 (2) of GDPR in its version of 11 June 2015.
[210] Article 17 of Directive 95/46/EC; Article 30 of GDPR in its version of 11 June 2015; Article 22 of Framework Decision 2008/977/JHA; Article 27 of DDPLE in its version of 29 June 2015.
[211] Article 23 of GDPR in its version of 11 June 2015; Article 19 of DDPLE in its version of 29 June 2015.
[212] Article 22 (2) of Framework Decision 2008/977/JHA; Article 27 (2) of DDPLE in its version of 29 June 2015.
[213] Articles 31 and 32 of GDPR in its version of 11 June 2015; Articles 28 and 29 of DDPLE in its version of 29 June 2015.
[214] Council of Europe, Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, 28 January 1981, CETS No. 108 (in the following: Convention No. 108); Council of Europe, Recommendation R (87) 15 of the committee of ministers to member states regulating the use of personal data in the police sector, adopted on 17 September 1987 (in the following: CoE Recommendation R (87) 15).

protection and LE related matters until the Lisbon Treaty entered into force at the end of 2009.[215] Prior to the adoption of the Lisbon Treaty the Court was hindered with the establishment of EU principles in this area due to the constitutional divide into three pillars, which was finally abolished with the Treaty. The competence of the ECtHR included this policy field allowing it to develop central principles in this particular area, whereas the control of European Courts was limited to the restricted competences of the former EU and EC treaties.

Nowadays, Articles 7 and 8 CFR build overarching fundamental rights in EU law covering all policy areas, including LE matters. Additionally, the accession of the EU to the ECHR is provided in Article 6 TEU and paragraph (3) of the same article declares that the fundamental rights of the ECHR constitute general principles of EU law. In addition, EU fundamental rights corresponding to the rights of the ECHR, shall have the same meaning and scope of the Convention's rights.[216] The principles developed by the ECtHR with regard to data protection and privacy within the framework of Article 8 ECHR in recent years are therefore of utmost importance for the interpretation of Articles 7 and 8 of the Charter.

2.3.1. Article 8 ECHR

Article 8 ECHR is the most important provision protecting data in the LE sector within the framework of the Council of Europe. It contains several guarantees surrounding the protection of privacy, including more specifically the rights to respect private and family life, home and correspondence. It reads as follows:

> Article 8 ECHR, right to respect for private and family life
>
> 1. Everyone has the right to respect for his private and family life, his home and his correspondence.
>
> 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.

For the purpose of this study, particular attention will be paid to the data protection guarantees in the LE sector developed by the ECtHR in its extensive case law in this area.[217] This section summarizes the most important principles which can be derived from these judgements.

2.3.1.1. Scope of Application of Article 8 ECHR and ECtHR case law

The scope of Article 8 ECHR is determined by Article 1 ECHR, obliging ECHR member states to guarantee "**everyone within their jurisdiction the rights and freedoms**" contained in the ECHR. The rights of the ECHR therefore apply to every person of the contracting state, including third country nationals, providing that they are subjected to the jurisdiction of one of the Convention's states.

Although data protection is not expressly mentioned in Article 8 ECHR, the Strasbourg Court repeatedly holds that the **protection of personal data is of fundamental**

[215] However, it repeatedly referred to the guarantees developed by the ECtHR with regard to Article 8 ECHR when data protection issues in internal market matters were the subject of EU cases.
[216] Article 52 (3) CFR.
[217] For a detailed analysis of the ECtHR's case law in this area, compare: Boehm, Information sharing and data protection in the Area of Freedom, Security and Justice, pp. 25-83; most of the findings in the following originate from this book.

importance to a person's enjoyment of his or her right to respect for private and family life within the framework of this article.[218] The term private life in Article 8 ECHR covers various actions and has a broad scope "that is not susceptible to exhaustive definition".[219] Within this scope, it is, since decades, widely recognized that data protection guarantees originated from this right, forming a vital part of it today. The scope of the right to data protection itself is equally broad and not further specified. In data protection cases, the ECtHR regularly stresses that the guarantees of Article 8 with regard to private life correspond to the guarantees of Convention No. 108, whose purpose it is to guarantee every individuals right to privacy with regard to data processing.[220] Limitations of the scope are therefore difficult to find. Usually, the questions referred to the ECtHR must simply be in accordance with the two requirements mentioned in Convention No. 108, namely, that the case must deal with *information* and the latter must be of *personal nature*.[221]

Regarding the obligations of the Convention's member states, Article 1 ECHR, read together with Article 34 ECHR, restricts the states liability to governmental actions. This includes cases in which a state is held responsible for failing its positive obligation (i.e. cases in which the state interferes with a Convention's right by omitting to do something) to protect the individual against interferences from private actors. Such cases may have important legal effects on third parties.

2.3.1.2. Substantive Data Protection Guarantees of Article 8 ECHR in the LE sector

To examine whether data processing complies with Article 8 ECHR, the ECtHR applies a three-step test. In a first step, it verifies whether the data processing in question falls within the scope of Article 8 ECHR. Secondly, it asks whether there has been an interference with the rights stipulates in Article 8 (1) ECHR and, if so, in a third step it reviews whether this interference could be justified by the legitimate restrictions outlined in Article 8 (2) ECHR because it was in accordance with the law, pursued a legitimate aim and was necessary in a democratic society.

So far, the ECtHR considered the following activities in a broader LE context as a separate **interference** with Article 8 ECHR[222]:

- measures of secret surveillance and recording (e.g. *Klass v. Germany* and *Liberty and others v. the United Kingdom*);
- the mere existence of monitoring legislation (e.g. *Klass v. Germany*);
- the implementation measures of monitoring legislation, such as the installation of wiretapping instruments in an individual's house, in a prison or prison cell, or at the workplace, or the interception of telephone calls (e.g. *Khan v. the United Kingdom* or *Kopp v. Switzerland*);

[218] Compare: ECtHR for instance in *Z. v Finland*, Application no. 22009/93, Judgment of 25 February 1997, para 95; *Peck v. United Kingdom*, Application no. 44647/98, Judgment of 28 January 2003, para 78; *L.L. v France*, Application no. 7508/02, Judgment of 10 October 2006, para 43; *S. and Marper v the United Kingdom*, Application nos. 30562/04 and 30566/04, Judgment of 4 December 2008, para 103; See also: Moreham, European Human Rights Law Review, Issue 1, 2008, pp. 44-79.
[219] For instance, ECtHR, *Peck v. United Kingdom*, Application no. 44647/98, Judgment of 28 January 2003, para 57; *Niemietz v. Germany*, Application no. 13710/88, Judgment of 16 September 1992, para 29; *Pretty v. United Kingdom*, Application no. 2346/02, Judgment of 29 April 2002, para 61; *P.G. and J.H. v. United Kingdom*, Application no. 44787/98, Judgment of 25 September 2001, para 56.
[220] Compare: ECtHR, *Rotaru v. Romania*, Application no. 28341/954, Judgment of 4 May 2000, para 43; see also: *Amann v. Switzerland*, Application no. 27798/95, Judgment of 16 February 2000, para 65.
[221] Compare: Boehm, Information sharing and data protection in the Area of Freedom, Security and Justice, p. 30.
[222] Compare for a detailed analysis: Boehm, Information sharing and data protection in the Area of Freedom, pp. 33 to 45.

- the recording of a person's voice for further analysis (e.g. *P.G. and J.H. v. the United Kingdom*);
- the unwanted watching and recording in private or even public places, in the latter case, only if the activities were recorded (e.g. *Perry v. the United Kingdom*);
- the dissemination of photos or videos, if not foreseeable at the time of shooting (e.g. *Peck v. the United Kingdom*): the circumstances in which the material was taken, the foreseeability of dissemination at the time of recording and the situation in which the persons concerned were photographed/filmed have to be taken into account;
- the omission to prevent the dissemination of photos or videos taken in a private context (e.g. *Peck v. the United Kingdom*);
- the dissemination of medical records (e.g. *Z. v. Finland*);
- the denying of access to personal data (e.g. *Leander v. Sweden*, *C.G. and others v. Bulgaria*);
- the refusal to advise individuals of the full extent to which information was being kept about them on a security police register (e.g. *Segerstedt-Wilberg and others v. Sweden*)
- the collection, retention and storing of personal information (including telephone data or information relating to e-mail and internet usage), as well as its release, whereby even public information can fall within the scope of private life where it is systematically collected and stored in files held by the authorities (e.g. *Rotaru v. Romania*);
- the retention of cellular samples, DNA profiles and fingerprints in a database (e.g. *Marper v. the United Kingdom*);
- the different methods to gather and to collect personal information (e.g. *Weber and Saravia v. Germany*), and
- the transfer of personal data to third parties (e.g. *Malone v. the United Kingdom* or *Weber and Saravia v. Germany*).[223]

When the existence of an interference with Article 8 ECHR has been established, paragraph 2 of Article 8 ECHR comes into play. According to it, **the interference with the right to private life must satisfy three conditions to be considered legal**: (1) it must be in accordance with the law, (2) it must pursue one or more of the legitimate aims referred to in paragraph 2 and (3) it must be necessary in a democratic society in order to achieve these aims.[224] Article 8 (2) ECHR mentions the interests of national security, public safety or the economic well-being of the country, the prevention of disorder or crime, the protection of health or morals, or the protection of the rights and freedoms of others as legitimate aims. Typically, the ECtHR focuses on the third condition by carrying out a detailed proportionality assessment.

[223] ECtHR, *Klass v. Germany*, Application no. 5029/71, Judgment of 6 September 1978; *Khan v. the United Kingdom*, Application no. 35394/97, Judgment of 12 May 2000; *Kopp v. Switzerland*, Application no. 23224/94, Judgment of 25 March 1998; *P.G. and J.H. v. the United Kingdom*, Application no. 44787/98, Judgment of 25 September 2001; *Perry v. the United Kingdom*, Application no. 63737/00, Judgment of 17 July 2002; *Peck v. United Kingdom*, Application no. 44647/98, Judgment of 28 January 2003; *Z. v Finland*, Application no. 22009/93, Judgment of 25 February 1997; *Leander v. Sweden*, Application no. 9248/81, Judgment of 26 March 1987; *C.G. and others v. Bulgaria*, Application no. 1365/07, Judgment of 24 April 2008; *Segerstedt-Wiberg and others v. Sweden,* Application no. 62332/00, Judgment of 6 June 2006; *Rotaru v. Romania*, Application no. 28341/954, Judgment of 4 May 2000; *S. and Marper v the United Kingdom*, Application nos. 30562/04 and 30566/04, Judgment of 4 December 2008; *Weber and Saravia v. Germany*, Application no. 54934/00, Admissibility decision of 29 June 2006.

[224] ECtHR, *Weber and Saravia v. Germany*, Application no. 54934/00, Admissibility decision of 29 June 2006, para 80, *Liberty and others v. the United Kingdom*, Application no. 58243/00, Judgment of 1 July 2008, para 58.

(1) The criterion **"in accordance with the law"** goes well beyond the mere existence of some legal basis in domestic law. It requires a high quality of law.[225] The domestic legal rules must be adequately accessible by the individuals concerned, enabling them to understand whether their behaviour is adequate in the circumstances of the rules applicable to a given case.[226] The respective legal rule must be formulated with sufficient precision permitting the citizen to regulate his/her conduct and allowing to anticipate – if need be with appropriate advice –, to a degree that is reasonable in the situation, the consequences that a given action may entail.[227] Unspecified legal terms and concepts must be further defined by "settled case-law" or other legal rules specifying those terms.[228] As a final condition, the measure must be compatible with the rule of law.[229]

As certain data protection cases in LE regard secret surveillance measures the ECtHR developed a catalogue of protective principles, which have to be fulfilled by the legal basis in place to comply with the **foreseeability** criterion.

In the context of **secret measures of surveillance**, for instance in wiretapping cases, the nature of the offences which give rise to an interception order, the categories of people liable to have their telephones tapped, a limit on the duration of the tapping, the procedures to be followed for examining, using and storing the data obtained, rules regulating the transfer of data to other parties and the circumstances in which recordings have to be erased or the tapes have to be destroyed, have to be specified in a legal basis.[230]

A legal basis regulating **collection and storage of personal data for surveillance purposes** must include provisions about the type of information that might be recorded, the categories of people against whom surveillance measures might be taken, the circumstances in which such measures might be taken and the procedure to be followed. Further, the rules must include provisions regulating the age of information held, the length of time for which this information might be kept, explicit and detailed provisions concerning the persons authorised to consult the files, the nature of the files, the procedure to be followed and the use that might be made of the information thus obtained.[231]

If domestic law provides on the one hand, for a **wide discretion** for the implementation of surveillance measures, the law on the other hand, has to provide "adequate protection against abuse of power" and "the scope or manner of exercise" of the discretion conferred on the State, e.g. to intercept and examine external communications.[232] In addition, the provisions restricting the discretion must be accessible to the public.[233] In *Weber and Saravia v. Germany* the ECtHR concluded that it is possible for a State to publish certain details about the operation of a scheme of external surveillance without compromising national security by, amongst others, enacting detailed provisions about the use, storage,

[225] ECtHR, *Amann v. Switzerland*, Application no. 27798/95, Judgment of 16 February 2000, para 55.
[226] Ovey/White, p. 224.
[227] ECtHR, *Silver v. the United Kingdom*, Application no. 5947/72 and others, Judgment of 25 March 1983, paras 85-88.
[228] ECtHR, *Huvig v. France*, Application no. 11105/84, Judgment of 24 April 1990, para 28; *Kruslin v. France*, Application no. 11801/85, Judgment of 24 April 1990, para 35.
[229] ECtHR, *Kopp v. Switzerland*, Application no. 23244/94, Judgment of 25 March 1998, para 55.
[230] ECtHR, *Weber and Saravia v. Germany*, Application no. 54934/00, Admissibility decision of 29 June 2006, para 95; these criteria were developed at first in: ECtHR, *Huvig v. France*, Application no. 11105/84, Judgment of 24 April 1990, para 34 and *Kruslin v. France*, Application no. 11801/85, Judgment of 24 April 1990, para 35.
[231] ECtHR, *Rotaru v. Romania*, Application no. 28341/954, Judgment of 4 May 2000, para 57.
[232] ECtHR, *Liberty and others v. the United Kingdom*, Application no. 58243/00, Judgment of 1 July 2008, para 69.
[233] ECtHR, *Liberty and others v. the United Kingdom*, Application no. 58243/00, Judgment of 1 July 2008, paras 67 and 69.

communication and destruction of the obtained data.[234] In this case, the German legal basis included rules on the storage and destruction of the data involved, such as a six-month review period after which it had to verified, whether the data obtained were still necessary to achieve the purpose for which they had been obtained.[235] If that was not the case, the relevant data had to be destroyed and deleted from the files or access to them had to be blocked and the destruction had to be recorded in minutes.[236]

(2) If the interference is in accordance with the law, the respective measure must comply with the **legitimate aims** of paragraph 2 Article 8 ECHR. The aims include the interest of national security, public safety and the economic well-being of the country as well as the prevention of disorder or crime, the protection of health, morals or the rights and freedoms of others. Member states enjoy a wide margin of appreciation with regard to these aims.[237] Usually, the ECtHR does not consider the compliance with these aims in detail; instead it focuses on the subsequent necessity test that allows for a thorough analysis of the conflicting interests.

(3) In search for a balance between the interests of the Member States and the protection of fundamental rights, the ECtHR examines whether the challenged measures are **necessary in a democratic society**.

Regarding data protection principles in an LE environment, the ECtHR has developed a large amount of sophisticated case law in recent decades.[238] Consequently, this section will give a summarized overview of the principles established by the Strasbourg Court, instead of referring separately to every case in detail. Many cases concern questions relating to legislation enacted against terrorism, permitting surveillance, collection and storage of data, including the retention of information over long periods of time. The most important principles to be mentioned in the following stem in particular from the cases *S. and Marper v. the United Kingdom*, *Weber and Saravia v. Germany*, *Rotaru v. Romania*, *Leander v. Sweden*, *Liberty and Others v. United Kingdom*, and *M.K. v. France*.

Regarding the **storage of data for LE purposes**, the ECtHR insists on a **clear definition of the circumstances and limits of the storing** and the **use of the information** before processing.[239] The purpose limitation principle must be respected in an LE context as well, meaning that states must define which kind of data are to be stored and for which purposes the data should be used afterwards.[240] In *S. and Marper v. the United Kingdom*, the ECtHR developed important general principles in regards to minimum data protection standards in LE databases.[241] In view of the Strasbourg Court, the retention of fingerprints,

[234] ECtHR, *Weber and Saravia v. Germany*, Application no. 54934/00, Admissibility decision of 29 June 2006, paras 92 et seq.; *Liberty and others v. the United Kingdom*, Application no. 58243/00, Judgment of 1 July 2008, para 68.
[235] ECtHR, *Weber and Saravia v. Germany*, Application no. 54934/00, admissibility decision of 29 June 2006, para 100.
[236] ECtHR, *Weber and Saravia v. Germany*, Application no. 54934/00, Admissibility decision of 29 June 2006, para 100.
[237] Siemen, p. 151; Meyer-Ladewig, Article 8, p. 180, para 41.
[238] For details, compare: Boehm, Information sharing and data protection in the Area of Freedom, Security and Justice, p. 25-83.
[239] ECtHR, *Segerstedt-Wiberg and others v. Sweden,* Application no. 62332/00, Judgment of 6 June 2006, paras 88-92; *Liberty and others v. the United Kingdom*, Application no. 58243/00, Judgment of 1 July 2008, para 68; *Rotaru v. Romania*, Application no. 28341/954, Judgment of 4 May 2000, para 57; *Weber and Saravia v. Germany*, Application no. 54934/00, Admissibility decision of 29 June 2006, paras 116 and 127.
[240] ECtHR, *Weber and Saravia v. Germany*, Application no. 54934/00, Admissibility decision of 29 June 2006, para 116; *Rotaru v. Romania*, Application no. 28341/954, Judgment of 4 May 2000, para 57; see also: *Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria*, Application no. 62540/00, Judgment of 28 June 2007.
[241] ECtHR, *S. and Marper v. the United Kingdom*, Application nos. 30562/04 and 30566/04, Judgment of 4 December 2008, paras 66 to 125.

cellular samples and DNA profiles in a nationwide database violated Article 8 ECHR.[242] The ECtHR opposed "blanket and indiscriminate" data retention and clarified that the **presumption of innocence and the risk of stigmatization** stemming from the inclusion in an LE database, require a **different treatment of data of persons who have been convicted of an offence and those who have never been**.[243] **Distinctions must further be made between serious and less serious offences**, including the **age** of the suspected persons that has to be taken into account when storing data in LE databases.[244] If concrete surveillance measures are directed towards individuals, the surveillance measure must be limited to specific categories of individuals and cannot be directed against practically everybody.[245] Moreover, the **persons and authorities authorized to consult the files** must be defined before the data are processed in an LE context.[246]

The ECtHR considers **effective time limits** for the retained data as an essential guarantee following from the respect for Article 8 ECHR.[247] **Independent reviews** of LE databases and **adequate and effective safeguards against abuse**, including **effective remedies**, are crucial elements to guarantee compliance with the rule of law.[248] In particular, **independent oversight** must exist to verify whether the retention is (still) justified.[249] When carrying out this verification, criteria such as "the seriousness of the offence, previous arrests, the strength of the suspicion against the person and any other special circumstances" need to be taken into account.[250] In the recent *M.K. v. France* case the Strasbourg Court **opposed lengthy retention periods and ineffective provisions on deletion**. More concretely, the French database, which was subject to the case, provided for a 25-year retention period with the possibility for deletion of data, if they became unnecessary for the purpose of the database. The ECtHR clarified that the purpose for storing therefore correlated with the deletion provision. However, the database's purpose barely referred to the collection of as much data as possible rendering the deletion provision ineffective.[251] Such "theoretical and illusory" data retention periods are not "practical and effective" and are therefore considered as excessive and not in line with Article 8 ECHR.[252] The ECtHR's finding that provisions restricting the deletion of data to cases in which they are not necessary for the purpose of the database anymore, without providing for another practical and effective possibility of deletion during the retention period, violate Article 8 ECHR, is of fundamental importance for the LE sector. It signifies that even if states limit the retention period, there must be an effective possibility to delete the data during this period to comply with Article 8 ECHR.

[242] ECtHR, *S. and Marper v. the United Kingdom*, Application nos. 30562/04 and 30566/04, Judgment of 4 December 2008, para 125.
[243] ECtHR, *S. and Marper v. the United Kingdom*, Application nos. 30562/04 and 30566/04, Judgment of 4 December 2008, paras 119 and 122.
[244] ECtHR, *S. and Marper v. the United Kingdom*, Application nos. 30562/04 and 30566/04, Judgment of 4 December 2008, para 119; compare also *Segerstedt-Wiberg and others v. Sweden,* Application no. 62332/00, Judgment of 6 June 2006, paras 89 to 92.
[245] ECtHR, *Segerstedt-Wiberg and others v. Sweden,* Application no. 62332/00, Judgment of 6 June 2006, paras 88-92; *Liberty and others v. the United Kingdom*, Application no. 58243/00, Judgment of 1 July 2008, para 68; *Rotaru v. Romania*, Application no. 28341/954, Judgment of 4 May 2000, para 57; *Weber and Saravia v. Germany*, Application no. 54934/00, Admissibility decision of 29 June 2006, paras 116 and 127.
[246] ECtHR, *Rotaru v. Romania*, Application no. 28341/954, Judgment of 4 May 2000, para 57.
[247] ECtHR, *S. and Marper v. the United Kingdom*, Application nos. 30562/04 and 30566/04, Judgment of 4 December 2008, para 119 and *Segerstedt-Wiberg and others v. Sweden,* Application no. 62332/00, Judgment of 6 June 2006, paras 90-92.
[248] ECtHR*, Rotaru against Romania*, Application no. 28341/95, Judgment of 4 May 2000, paras 55-63; *Segerstedt-Wiberg and others v. Sweden,* Application no. 62332/00, Judgment of 6 June 2006, para 121.
[249] ECtHR, *S. and Marper v. the United Kingdom*, Application nos. 30562/04 and 30566/04, Judgment of 4 December 2008, para 119.
[250] ECtHR, *S. and Marper v. the United Kingdom*, Application nos. 30562/04 and 30566/04, Judgment of 4 December 2008, para 119.
[251] ECtHR, *M.K v. France*, no. 19522/09, Judgement of 18 April 2013, para 39.
[252] ECtHR, *M.K v. France*, no. 19522/09, Judgement of 18 April 2013, para 44.

As technological developments facilitate the ability to **exchange data** the risks for individuals concerned with having their data stored in various databases increases. Therefore, the ECtHR developed procedural rules for the exchange of data between LE authorities. In particular, in the admissibility decision *Weber and Saravia v. Germany* the Strasbourg Court used the opportunity to clarify which guarantees would be in accordance with Article 8 ECHR. More concretely, it stressed that **the types of offences on behalf of which data transmission between LE agencies is permitted must be restricted**.[253] If data are transferred to other LE authorities, the data must be **marked and remain connected to the purposes** which had justified their collection.[254] Further, the **transmission of data must be recorded in minutes** to establish safeguards against abuse.[255]

In the *Leander v. Sweden* case dating back to 1987, the ECtHR referred to the **design and conditions of an access procedure** to data stored in an LE database. It was satisfied with the Swedish procedure that entailed explicit and detailed conditions relating to a list of the authorities to which information may be communicated as well as the circumstances in which such communication may take place and the procedure to be followed.[256] The findings were later confirmed in *Weber and Saravia v. Germany*. In some cases, if access is refused, even the reasons substantiating the refusal of access must be revealed.[257]

A further important principle in the LE context relates to the **retrospective notification of individuals subjected to surveillance measures**.[258] According to ECtHR, notification is directly linked to the **effectiveness of remedies** before courts and therefore to the existence of effective safeguards against the abuse of monitoring powers.[259] Due to this important link, notification should be carried out as soon as possible after the termination of the measure.[260]

Summarizing, the extensive ECtHR case law on data protection principles in LE mirrors the significance the Strasbourg Court dedicates to the development of substantive data protection rights of individuals in an LE context. It has established clear and detailed rules over the years, which serves the Convention's member states as well as the EU legislators guiding principles in similar contexts. Only recently, the CJEU made use of these principles in a famous data retention judgement.[261]

2.3.2. Article 13 ECHR

In connection with a violation of Article 8 ECHR, a breach of Article 13 ECHR is often also claimed. This right guarantees that "Everyone whose rights and freedoms as set forth in this Convention are violated shall have an effective remedy before a national authority…".

[253] ECtHR, *Weber and Saravia v. Germany*, Application no. 54934/00, Admissibility decision of 29 June 2006, para 129.
[254] ECtHR, *Weber and Saravia v. Germany*, Application no. 54934/00, Admissibility decision of 29 June 2006, para 121.
[255] ECtHR, *Weber and Saravia v. Germany*, Application no. 54934/00, Admissibility decision of 29 June 2006, para 127.
[256] ECtHR, *Leander v. Sweden*, Application no. 9248/81, Judgment of 26 March 1987, para 55.
[257] ECtHR, *C.G. and others v. Bulgaria*, Application no. 1365/07, Judgment of 24 April 2008, paras 46 and 47.
[258] Boehm/de Hert, European Journal of Law and Technology, Vol. 3, No. 3, 2012 and Boehm/de Hert, Yearbook of the Digital Enlightenment Forum 2012, pp. 19-39.
[259] ECtHR, *Weber and Saravia v. Germany*, Application no. 54934/00, Admissibility decision of 29 June 2006, para 135: "since there is in principle little scope for recourse to the courts by the individual concerned unless the latter is advised of the measures taken without his or her knowledge and thus able to challenge their legality retrospectively".
[260] ECtHR, *Weber and Saravia v. Germany*, Application no. 54934/00, Admissibility decision of 29 June 2006, para 135.
[261] Compare above, section 2.1.3.3.

Article 13 ECHR is an auxiliary right whose violation may only be invoked together with a violation of a substantive right.

In LE related cases, Article 13 ECHR is typically invoked if domestic law does not provide for a **remedy for violations of data protection rights**.[262] In those cases, the Strasbourg Court analyses separately and additionally to Article 8 ECHR, whether domestic law complies with the guarantees of Article 13 ECHR. The right to an effective remedy is also violated, if an oversight body monitoring an LE database admittedly exists, but has no competence to order destruction, rectification or erasure of information kept in the database.[263] In this way, Article 13 ECHR complements the protection stemming from Article 8 ECHR by assuring the **effective enforcement of erasure and notification rights**. Moreover, the **right to notification and appeal**, even after secret surveillance measures, can also be derived from right to effective remedy.[264] Neglecting to notify individuals in the aftermath of surveillance contradicts Article 13 ECHR, as it hinders those seeking redress in regards to the secret surveillance measures performed.[265]

2.3.3. Convention No. 108 and Recommendation No. R (87) 15

The Council of Europes' Convention No. 108 for the Protection of Individuals with regard to the Automatic Processing of Personal Data is a further development of Article 8 ECHR, applicable to data processing in the public as well as in the private sector.[266] The European Communities acceded Convention No. 108 in June 1999.[267] It is briefly mentioned here, since some EU instruments, including those in the LE sector, refer to it.[268] Convention No. 108 includes the most important data protection principles, such as purpose limitation, fair and lawful processing and the requirements of adequacy and relevance.[269] Further, it entails rules on "special categories" of data and a sanction and remedy system for data protection violations.[270] Information, rectification and erasure rights for individuals are equally specified.[271] However, Convention No. 108 does not include rules on the transfer of data to third states. Therefore the Convention was enhanced by an additional protocol on supervisory authorities and trans-border data flows in 2001.[272] It establishes a similar adequacy mechanism as Directive 95/46/EC. Due to the more specific rights entailed in Directive 95/46/EC, the relevance of Convention No. 108 in EU law is minor. However, it

[262] ECtHR, *Peck v. the United Kingdom*, Application no. 44647/98, Judgment of 28 January 2003, paras 91-114; *Kirov v. Bulgaria*, Application no. 5182/02, Judgment of 22 May 2008, paras 48 to 58.
[263] ECtHR, *Segerstedt-Wiberg and others v. Sweden,* Application no. 62332/00, Judgment of 6 June 2006, para 121.
[264] ECtHR, *Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria*, Application no. 62540/00, Judgment of 28 June 2007, paras 96-103; *Kirov v. Bulgaria*, Application no. 5182/02, Judgment of 22 May 2008, paras 48-58; *Klass v. Germany*, Application no. 5029/71, Judgment of 6 September 1978, paras 69-70; *Weber and Saravia v. Germany*, Application no. 54934/00, Admissibility decision of 29 June 2006, para 157; *Rotaru v. Romania*, Application no. 28341/954, Judgment of 4 May 2000, para 57.
[265] ECtHR, *Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria*, Application no. 62540/00, Judgment of 28 June 2007, para 101.
[266] Convention No. 108.
[267] Council of Europe, Amendments to the Convention for the protection of individuals with regard to automatic processing of personal data (ETS No. 108) allowing the European Communities to accede, adopted by the Committee of Ministers on 15 June 1999, available at: http://conventions.coe.int/treaty/en/Treaties/Html/108-1.htm.
[268] Recital (11) of Directive 95/46/EC; Article 14 of Council Decision 2009/426/JHA of 16 December 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 L 138, 4.6.2009, p. 14 – 32; Article 27 of Europol Decision 2009/371/JHA etc.
[269] Article 5 (a) to (e) of Convention No. 108.
[270] Articles 6, 8 and 10 of Convention No. 108.
[271] See Article 8 of Convention No. 108.
[272] Council of Europe, Additional Protocol of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows, 8 November 2001, available at: http://conventions.coe.int/treaty/en/Treaties/Html/181.htm.

can play a role in the LE sector for activities which are not covered by the Framework Decision 2008/977/JHA.[273]

Another instrument of the Council of Europe includes guidelines for data protection in the LE sector. **Recommendation No. R (87) 15** regulating the use of personal data in the police sector, already adopted in 1987, represents a quite comprehensive framework for data protection principles for LE which is still being referred to by a number of EU instruments dealing with the use of personal data in a police context.[274] Additionally, most of the EU Member States have implemented the principles into national law.[275]

The first principle of eight, requires **independent control and supervision established outside the police sector**. It refers to some basic tasks the supervisory authorities should be equipped with, including consultation and notification requirements with regards to police files. Supervisory authorities should also be empowered to check regularly the quality of police data.[276] Further, Recommendation No. R (87) 15 entails the **purpose limitation principle**, requiring data to be held only for reasons such as the prevention of a real danger or the suppression of specific criminal offences.[277] Importantly, the second principle of Recommendation No. R (87) 15 mentions a **notification requirement** for individuals concerned, as soon as police activities are no longer prejudiced by this task. **Differentiating the categories of data** in police files is equally required, just as a **strict purpose limitation provision regarding the transfer of police data to other parties**, including private actors.[278] For instance, transfer of police data to foreign authorities should be restricted to police bodies and should only be allowed if there is a clear legal provision under national or international law and only, if the accuracy of the data has been verified before the transfer.[279] The initial police related purpose should not be altered.[280] Moreover, individuals should be empowered with **access, rectification and erasure rights**.[281] If access is refused, **appeal to an independent body** should be possible.[282] The seventh principle requires **time limits for retention and final deletion** of data. Recommendation No. R (87) 15 even mentions criteria that should be taken into account when establishing the time limit: the need to retain data in light of the conclusion of an inquiry into a particular case, a final judicial decision, in particular an acquittal, rehabilitation, spent convictions, amnesties, the age of the data subject and particular categories of data.[283] Finally, principle eight requires data security measures to be in place to ensure appropriate technical protection.

2.4. Key Findings

Data protection is recognized as a fundamental right in EU law since the entering into force of the Lisbon Treaty. EU law provides for a comprehensive data protection framework,

[273] Kranenborg, in: Peers/Hervey/Kenner/Ward, Article 8, p. 238.
[274] CoE Recommendation R (87) 15, referenced by the Europol Decision 2009/371/JHA (Article 27 and recital 14) the Schengen instruments (Articles 115 and 117 of The Schengen acquis - Convention implementing the Schengen Agreement of 14 June 1985 between the Governments of the States of the Benelux Economic Union, the Federal Republic of Germany and the French Republic on the gradual abolition of checks at their common borders OJ L 239, 22.9.2000, p. 19–62) and the Prüm Convention (Article 34 Prüm Convention, available at: http://ec.europa.eu/anti_fraud/documents/data-protection/dpo/prumtr.pdf).
[275] Compare: Cannataci/Caruana, available at: http://www.statewatch.org/news/2013/oct/coe-report-data-privacy-in-the-police-sector.pdf.
[276] Principle 7.2. of CoE Recommendation R (87) 15.
[277] Principles 2 and 4 of CoE Recommendation R (87) 15.
[278] Principle 5 of CoE Recommendation R (87) 15.
[279] Principles 5.4. and 5.5. of CoE Recommendation R (87) 15.
[280] Principle 5.5.iii. of CoE Recommendation R (87) 15.
[281] Principle 6 of CoE Recommendation R (87) 15.
[282] Principle 6.6. of CoE Recommendation R (87) 15.
[283] Principle 7.1. of CoE Recommendation R (87) 15.

including in the LE sector. Case law of the ECtHR, as well as of the EU courts, has established several important data protection principles, which are often codified in EU secondary law. The latter has to comply with primary law, in particular with Articles 7 and 8 of the Charter and can be declared invalid, if it contradicts primary law, as recently seen in the data retention case. The EU data protection canon includes several core principles, which also apply in the LE sector. They refer to, amongst others, rules on data quality standards, on sensitive data, independent supervision, the purpose limitation principle, strict rules on inter-agency exchange and the transfer of data to third states, time limits for the retention of data, effective judicial review and access possibilities, independent oversight, proportionality elements, notification requirements after surveillance and data breaches, as well as rules on automated decisions and data security as well as technical protection. These principles can be lawfully restricted in an LE context. However, possible restrictions have to pass a strict proportionality test which considers individual rights and are subject to a substantive judicial review.

The recently decided data retention case underscored the importance of data protection principles, and also relates to an LE context. It clarified that infringements in data protection cases are independent of personal discomfort of the persons affected. The collection and retention of data, as well as the possibility of access by LE authorities each constituted separate infringements of Articles 7 and 8 CFR, which required a strict necessity and proportionality test.[284] The comprehensive targeting of EU citizens through data retention measures was considered as a "particularly serious" and "wide-ranging" interference of fundamental rights. The Court opposed blanketed and indiscriminate mass retention of data and also clarified that the mass access to content of communications would violate the essence of rights and could therefore not even be subject to a possible justification.

Another very important aspect of the case concerns the situation in which data originally collected for other purposes are later used for LE purposes. The Court required a connection between a threat to public security and the data retained for LE purposes.[285] This link is of a particular importance in an LE context, as it significantly influences the relationship between private and public actors, meaning that LE agencies are only allowed to access data which has been collected for other purposes in individual cases.

Rules on the transfer of data to third states are currently subject to discussion at an EU policy level, with the adequacy of the level of protection in third states still playing a decisive role. Existing transfer arrangements, such as the safe harbor regime allow for wide ranging exemptions and are most likely no loner in line with EU fundamental rights. Newly proposed rules in the GDPR as well as in the DDPLE seem to partly improve the currently unsatisfying situation.

In summary, EU data protection guarantees additionally apply to the LE sector and build a comprehensive framework consisting of various legal sources in EU and ECHR law that underpin the constitutional protection. Some of the guarantees in recent case law, which stem from the interpretation of the Charter, still need to be integrated into existing agreements, in particular regarding arrangements that regulate the transfer of data to the US. Ongoing negotiations relating to an "Umbrella Agreement" must therefore respect the existing EU data protection guarantees illustrated in detail in this section.

[284] CJEU, C-293/12 and C-594/12 *Digital Rights Ireland*, para 35.
[285] CJEU, C-293/12 and C-594/12 *Digital Rights Ireland*, para 59.

3. US DATA PROTECTION GUARANTEES IN LAW ENFORCEMENT

To illustrate US data protection guarantees in LE, the author of this study was referred to the assessment made in a corresponding research paper prepared for the LIBE committee by *Prof. Francesca Bignami* in May 2015 with the title: "The US legal system on data protection in the field of law enforcement - Safeguards, rights and remedies for EU citizens". This section will therefore be considerably shorter than the EU section as it will partially base its findings on the *Bignami* study whilst, at the same time, avoiding a detailed repetition of its results. Nonetheless, in order to subsequently carry out a comparison between EU and US data protection guarantees in LE, it is essential to briefly illustrate the most important US data protection guarantees (sections 3.1., 3.2. and 3.3.) and its restrictions (section 3.4.). As changes to the legislative framework were recently introduced through the Draft Judicial Redress and the USA FREEDOM Act, the study will include a brief assessment of these changes.

3.1. Fourth Amendment to the Constitution

Constitutional data protection guarantees in the LE context are very limited. The main constitutional source serving as a basis for legal protection against intrusive law enforcement actions in this field is the Fourth Amendment to the Constitution. Its guarantee of the "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures" is understood to encompass certain data attributed to a person, such as telephone or banking records.[286] However, it only applies in cases where the individual has a "legitimate expectation of privacy".[287] This concept has been comprehensively reduced to exclude all cases where an individual has voluntarily turned over the information in question to third parties, such as its bank or telephone service provider, before the LE gets hold thereof (Third Party Doctrin).[288] This effectively excludes wide areas of personal data from Fourth Amendment protection altogether, such as visited websites, e-mail addressees, dialed phone numbers, as well as utility, banking, and education records.[289] On a personal level, the Fourth Amendment does generally not apply to foreign citizens and residents, such as EU citizens who are not resident in the US.[290]

In the limited cases where the Fourth Amendment guarantees apply, they may be justified by "reasonable" governmental interests.[291] If the guarantees are found to prevail, remedies amount to suppression as evidence in criminal proceedings and civil remedies such as damages.[292]

It is interesting to note that – in spite of its limits summarized above – the Fourth Amendment has recently been applied by the judiciary in a judgement that has been

[286] For telephone records see *Smith vs. Maryland*, 442 U.S. 735 (1979); for banking records see *United States vs. Miller*, 425 U.S. 435 (1976).
[287] *Katz vs. United States*, 389 U.S. 347 (1967).
[288] It is noted that courts may scrutinise this broad exemption in light of the changing electronic and technical environment, cf. *ACLU vs. Clapper*, No. 14-42 (2nd Cir. May 7, 2015). However, this development has yet to crystallize in practice.
[289] Thompson, p. 1.
[290] *United States vs. Verdugo-Urquides*, 494 U.S. 1092 (1990).
[291] Bignami, p. 10.
[292] Bignami, p. 10.

interpreted as creating a potential "right to deletion" of outdated data held by law enforcement agencies.[293]

3.2. Privacy Act 1974

The Privacy Act of 1974 aims to regulate personal data processing in the US.[294]

It regulates the collection, use, and disclosure of many types of personal information, described as a "record" kept on an individual: "including, but not limited to, his education, financial transactions, medical history, and criminal or employment history" containing "his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph".[295]

Its addressees are in principle all types of federal agencies, including law enforcement agencies, which excludes state or local agencies and private entities.[296]

The subject matter of the Privacy Act of 1974 is limited to those records kept in a "system of records", i.e. a data base described as a "group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual".[297] This should cover most common uses of data in the law enforcement context, but likely excludes data mining activities.[298] Only a few types of specifically sensitive data are treated preferentially, in particular First Amendment rights, relating to freedom of expression and association, and medical and psychological records.[299]

The application of the Act is further limited to US citizens or aliens with permanent residence in the US.[300] EU citizens are hence excluded, unless they reside permanently in the US.

Concerning the disclosure rules, "no agency shall disclose any record which is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains."[301] However, the application of this rule is subject to twelve explicitly listed exemptions, most prominently for "routine use" and for disclosure to other US agencies and governmental jurisdictions "for a civil or criminal law enforcement activity".[302] This largely reduces the impact of this guarantee for an individual in the LE context.

An individual enjoys the right to access and review its data and to retain a copy thereof; it may request the revision thereof if it believes the data is not accurate, relevant, timely or

[293] *United States v. Ganias*, No. 12-240 (2d Cir. 2014); See also Fourth Amendment — Search and Seizure and Evidence Retention — Second Circuit Creates a Potential "Right to Deletion" of Imaged Hard Drives. — *United States v. Ganias,* 755 F. 3d 125 (2d Cir. 2014), 128 Harv. L. Rev. 743, available at: http://harvardlawreview.org/2014/12/united-states-v-ganias.
[294] Privacy Act of 1974, enacted on 31 December 1974, Pub. L. 93-579; Cf. Bignami, pp. 10 et seq.
[295] 5 U.S.C. § 552a(a)(4).
[296] 5 U.S.C. § 552a(a)(1).
[297] 5 U.S.C. § 552a(a)(5).
[298] Bignami, p. 11.
[299] 5 U.S.C. § 552a(e)(7) and 5 U.S.C. § 552a(f)(3).
[300] 5 U.S.C. § 552a(a)(2).
[301] 5 U.S.C. § 552a(b).
[302] 5 U.S.C. § 552a(b)(3) and (7).

complete.[303] However, access is excluded to any information "compiled in reasonable anticipation of a civil action or proceeding", thus effectively limiting access rights.[304]

Transparency requirements include the obligation of each agency to inform individuals from which they request data of the authorization of such a request, the principle purpose of the data collection, the routine uses and the effects on such individual. In addition, a notice must be published in the Federal Register of the existence and character of a system of records set up by an agency.[305] Transparency obligations are however partly limited by a reasonableness test for the benefit of the agency concerned.[306]

Agencies are obliged to maintain in their records only such information about individuals "as is relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or by executive order of the President".[307] They are held to ensure accuracy, relevance, timeliness, and completeness of records, "as is reasonably necessary to assure fairness to the individual" concerned.[308] The relevance and necessity elements can be understood as a sort of proportionality test.[309] However, the Act does not explicitly mention such a term or require a balancing of interests.

The reference to "a purpose" hints at a purpose limitation principle, but has been applied by the courts in a rather weak fashion, stressing that "a" (rather understood as "any") legitimate purpose of the relevant agency is sufficient.[310] A stricter interpretation seems to be applied by the courts in the field of "routine use" of records, which requires a "use of such record which is compatible with the purpose for which it was collected."[311] Courts decide on a case-by-case basis whether such a principle is violated.[312] Because it is only applied in the context of routine use, it nevertheless falls short of being a general legal principle.

Finally, agencies are obliged to maintain security and confidentiality of the records they keep.[313]

No provisions exist regarding data retention periods.[314]

In addition, the rights of individuals and obligations of the agencies are broadly limited in the LE context by several sets of general and specific exemptions.[315] This basically excludes records maintained by the CIA and by law enforcement agencies, including their crime prevention activities, and other investigatory material from the vast majority of such rights and obligations, for example from the relevance and necessity test, the duty of accuracy, relevance, timeliness and completeness, access and correction rights and the availability of

[303] 5 U.S.C. § 552a(d)(1) and (2).
[304] 5 U.S.C. § 552a(d)(5).
[305] 5 U.S.C. § 552a(e)(3) and (4).
[306] 5 U.S.C. § 552a(e)(5), (6) and (8).
[307] 5 U.S.C. § 552a(e)(1).
[308] 5 U.S.C. § 552a(e)(5) and (6).
[309] Bignami, p. 11.
[310] *Reuber v. United States*, 829 F.2d 133, 138-39.
[311] 5 U.S.C. § 552a(a)(7).
[312] The United States Department of Justice, *Overview of the Privacy Act of 1974, Conditions of Disclosure to Third Parties, Part 3.2, 5 U.S.C. § 552a(b)(3) (routine uses)*, available at: http://www.justice.gov/opcl/conditions-disclosure-third-parties#routine.
[313] 5 U.S.C. § 552a(e)(10).
[314] Bignami, p. 12.
[315] 5 U.S.C. § 552a(j) and (k); see also: The United States Department of Justice, Overview of the Privacy Act of 1974, Ten Exemptions, available at: http://www.justice.gov/opcl/ten-exemptions.

civil remedies.[316] Not surprisingly, the FBI routinely and comprehensively invokes both general and specific exemptions.[317]

In addition to the criminal sanctions for agency officers or employees violating the guarantees contained in subsection 5 U.S.C. § 552a(i) of the Act, civil remedies are the main tool of individuals who want to invoke a violation of their rights under the Act.

The Act guarantees four types of legal action available to individuals.[318] They are available when an agency (A) makes a determination "not to amend an individual's record in accordance with his request, or fails to make such review in conformity with" the applicable procedural rules; (B) refuses to comply with an individual's request to access its records; (C) "fails to maintain any record concerning any individual with such accuracy, relevance, timeliness, and completeness as is necessary to assure fairness in any determination relating to the qualifications, character, rights, or opportunities of, or benefits to the individual that may be made on the basis of such record, and consequently a determination is made which is adverse to the individual"; or (D), quite generally, "fails to comply with any other provision of this section" [i.e. the Act], "or any rule promulgated thereunder, in such a way as to have an adverse effect on an individual".

Under these four types of legal action, if found in favor of the individual, courts shall grant the individual (A) an amendment of the record relating to the individual, plus attorney's fees and other litigation costs; (B) access to its records, plus attorney's fees and other litigation costs; and (C) and (D) actual damages with a minimum of USD 1,000, plus the cost of the action together with reasonable attorney fees.

Finally, it should be mentioned that the Act foresees the installation of internal officers overseeing compliance with the privacy obligations, which are however, by their very nature as internal officers, not vested with the same structural independence and powers as the external European Data Protection Authorities.[319]

3.3. Draft Judicial Redress Act of 2015

The draft Judicial Redress Act of 2015 (Draft Bill) aims to mitigate a main procedural shortcoming of the Privacy Act of 1974, its non-applicability to non-US citizens or residents.[320] Citizens of the EU and of other so-called "covered countries", which are defined as "covered persons", may now make use of certain civil remedies granted by the Privacy Act of 1974.[321] It must however be noted that the Draft Bill lags significantly behind granting equal rights to US and EU citizens.

Leaving aside the structural shortcomings of the Draft Bill, which begins directly with procedural rights thus leaving the material rights and guarantees of EU citizens somewhat unclear and open to interpretation, it should be noted that the field of application of the

[316] It should be noted that, as described above, the application of the disclosure rules and the specific protection of First Amendment related records are already excluded in the LE context without the necessity to invoke the exemptions under 5 U.S.C. § 552a(j) and (k); see 5 U.S.C. § 552a(b)(7) and 5 U.S.C. § 552a(e)(7).
[317] Bignami, pp. 12 et seq.
[318] 5 U.S.C. § 552a(g).
[319] Bignami, p. 12.
[320] Draft Judicial Redress Act, House of Representatives Bill H.R. 1428 of 18 March 2015; Senate Bill S. 1600 of 17 June 2015 (in the following: Judicial Redress Act).
[321] Section 2(a) of the Judicial Redress Act refers to 5 U.S.C. § 552a(g)(1), subparagraphs (A), (B) and (D), not however subparagraph (C).

civil remedies available to "covered persons" is narrowed down to so-called "covered records".[322]

These are only those records maintained by a US agency; such terms are defined in the Privacy Act of 1974[323], which are "transferred (A) by a public authority of, or private entity within, a country or regional economic organization, or member country of such organization, which at the time the record is transferred is a covered country; and (B) to a designated Federal agency or component for purposes of preventing, investigating, detecting, or prosecuting criminal offenses."[324] This means that any data relating to EU citizens, which is not actively transferred by the public authorities or private entities in the EU to US authorities, but otherwise retrieved or collected by these US authorities is not covered. Likewise, only data transferred to "designated Federal agencies and components" is covered, while the designation of such agencies lies in the discretion of the US Attorney General and is not subject to judicial review.[325] Such designation is, with the exception of the Department of Justice, also subject to the approval of the head of the agency concerned and must, among other things, be in the law enforcement interests of the United States, which is also not further defined and leaves room for utmost discretion.[326] It remains to be seen which agencies will finally be covered, but these rules allow for wide-ranging exemptions. In any case, data transferred to non-designated agencies is not covered.

From the analysis of the Draft Bill, it also seems to be the case that data is not covered when the transfer took place before a country became a "covered country" and that a "covered person" loses its right to sue if the designation of its home country as a "covered country" is revoked by the Attorney General.[327]

Concerning the available civil remedies, it must firstly be noted that only three out of the four remedies of the Privacy Act of 1974, 5 U.S.C. § 552a(g), are available to "covered persons". The remedy under 5 U.S.C. § 552a(g)(1)(C) is not covered at all, which grants actual damages, costs and attorney fees, if it is found that any agency "fails to maintain any record concerning any individual with such accuracy, relevance, timeliness, and completeness as is necessary to assure fairness in any determination relating to the qualifications, character, rights, or opportunities of, or benefits to the individual that may be made on the basis of such record and consequently a determination is made which is adverse to the individual." Secondly, the general remedy under 5 U.S.C. § 552a(g)(1)(D), which grants the same rights where an agency quite generally "fails to comply with any other provision of this section, or any rule promulgated thereunder, in such a way as to have an adverse effect on an individual" is narrowed down by the Draft Bill to cases of "disclosures intentionally or wilfully made in violation of section 552a(b)", which relates to the conditions of the disclosure of data.[328] This excludes not only e.g. grossly negligent disclosures, but any and all other potential violations of the covered person's rights. Thirdly, the procedural remedies under 5 U.S.C. § 552a(g)(1)(A) and (B) for correction and access to data and attorney fees and costs available in case an agency denies amendment of data or denies access to such data are only available against a "designated Federal agency or component", not against all other agencies.[329]

[322] On the structural deficits see Bignami, p. 13.
[323] 5 U.S.C. § 552a(a)(1) and (4).
[324] Section 2(h)(4) of the Judicial Redress Act.
[325] Sections 2(e) and (f) of the Judicial Redress Act.
[326] Section 2(e)(2)(B) of the Judicial Redress Act.
[327] Sections 2(a), (d) and (h) of the Judicial Redress Act.
[328] Section 2(a)(1) of the Judicial Redress Act.
[329] Section 2(a)(2) of the Judicial Redress Act.

Finally, the main paradox of the Draft Bill is that it only covers data transferred "for purposes of preventing, investigating, detecting or prosecuting criminal offences", i.e. LE purposes, while at the same time pointing out twice that the rights of the covered persons are subject to "the same limitations, including exemptions and exceptions" applicable to an individual under the Privacy Act of 1974.[330] Given the broad exemptions available in the LE context under the Privacy Act of 1974, as described in section 3.2 above, the already narrow field of application of the Draft Bill may be comprehensively diminished if these exemptions are applied. Even though the responsible US District Court for the District of Columbia upheld some restrictions to the application of these exemptions, civil remedies against, e.g., the FBI's Data Warehouse System, would be reduced to those against intentional or wilful illegal disclosures which cause actual damages of the EU citizen concerned.[331] This is however only in those cases where all the other conditions outlined above are fulfilled, in particular that "covered records" are concerned at all.

3.4. Restrictions of LE Data Protection Guarantees through ECPA, FISA and PATRIOT and USA FREEDOM Act

As seen above, US data protection guarantees already allow for broad exceptions in the LE sector. Numerous additional Acts permitting data collection by LE authorities for the purpose of criminal and/or national security investigations, which further restrict the general data protection guarantees, have been enacted in recent years. The amount of such Acts are overwhelming, making it difficult to give a comprehensive overview of the legal situation. The following section therefore limits its findings to the provisions of the most important restrictions included in the Foreign Intelligence Surveillance Act (FISA), the Electronic Communications Privacy Act (ECPA) and the USA PATRIOT Act (PATRIOT Act).[332] The latter Act primarily amended the FISA and the ECPA. However, many of its initially time-limited provisions have been reauthorized by successive Acts[333], most recently by the USA FREEDOM Act (FREEDOM Act).[334] A detailed analysis of these Acts can be found in the *Bignami* Study, which distinguishes between different methods of LE data collection, in particular between data collection for **ordinary criminal investigation** purposes and data collection for **national security investigations**. For reasons of clarity, this distinction will be maintained hereinafter.

3.4.1. Criminal Investigations under ECPA and FREEDOM Act

Bignami identifies three different LE methods to gather personal information in an ordinary criminal investigation context: (i) via the access to private databases and online resources, which include commercial and non-profit services; (ii) via administrative subpoenas for the production of documents; and (iii) via court orders under the ECPA.[335]

The use of the first instrument, **private databases and online resources,** which include commercial or non-profit services (e.g. commercial data brokers or social networks), seems

[330] Sections 2(a) and (c) of the Judicial Redress Act.
[331] Bignami, p. 14.
[332] Foreign Intelligence Surveillance Act of 1978, enacted on 25 October 1978, Pub. L. 95-511; Electronic Communications Privacy Act of 1986, enacted on 21 October 1986, Pub. L. 99-508; Uniting And Strengthening America By Providing Appropriate Tools Required To Intercept And Obstruct Terrorism Act Of 2001, enacted on 26 October 2001, Pub. L. 107-56.
[333] USA PATRIOT Improvement and Reauthorization Act of 2005, enacted on 6 March 2006, Pub. L. 109-177; USA PATRIOT Act Additional Reauthorizing Amendments Act of 2006, enacted on 6 March 2006; Pub. L. 109-178; FISA Sunsets Extension Act of 2011, enacted on 25 February 2011, Pub. L. 112-3; PATRIOT Sunset Extension Act of 2011, enacted on 26 May 2011, Pub. L. 112-14.
[334] Uniting And Strengthening America By Fulfilling Rights And Ensuring Effective Discipline Over Monitoring Act Of 2015, enacted on 2 June 2015, Pub. L. 114-23 (In the following: Freedom Act).
[335] Bignami, pp. 15 et seq.

to be mostly unregulated, but widely used.[336] The second possibility, **subpoenas** for testimony or for the production of documents are binding orders, which can be issued *inter alia* to enforce data collection activities by administrative authorities.[337] Numerous regulatory programs authorize LE agencies to use subpoenas while the conditions for the use of such instruments are minimal, usually only requiring a certain minimum relevance for the purpose of the investigation.[338] A third possibility is the use of **court orders under the ECPA** to carry out electronic surveillance and access electronic communications.[339] The ECPA consists of three Acts: the Wiretap Act, the Stored Communications Act, and the Pen Register Act and includes the conditions for electronic surveillance, interception and collection of metadata in the framework of ordinary criminal investigations.[340] The Acts lay down requirements and procedures for the access of LE authorities to records and communications, including electronic (e-mail, cloud services) and oral communications as well as metadata. Under the **Wiretap Act** LE authorities are allowed to intercept actual communications.[341] The **Stored Communications Act** allows for the accessing of records and communications held by providers of "electronic communications services" and "remote computing services", meaning e-mail or cloud services as well as internet service providers.[342] Data collected can relate to content (e-mails), metadata (information on e-mails) and subscriber records (name, address, payment details etc.).[343] The **Pen Register Act** allows for the surveillance of actual telephone and internet communications to collect metadata and requires a court order.[344]

While the Wiretap Act seems to entail the highest level of protection for the individuals concerned, the other Acts equally contain some basic protection rights, which vary according to the specific Act and the measure at stake. To access or intercept the protected communication, LE authorities need a court order, a search warrant or an administrative or judicial subpoena.[345] Interception in the framework of the Wiretap Act is **limited in time** and procedures to minimize the interception of communication, not otherwise subject to interception, should be executed.[346] The Wiretap Act and the Stored Communication Act provide for **notification** of the affected individual at some point after surveillance has been carried out.[347] Similar restrictions as the ones mentioned in EU law apply to this requirement. For instance, notification can be delayed, if the investigation would be jeopardized or a trial would be delayed.[348] An important provision of the Stored Communication Act is **18 U.S.C. 2709**, which allows the FBI to use a **National Security Letter (NSL)** to obtain non content subscriber information, toll billing records information or electronic communication transactional records from service providers for an investigation in international terrorism or clandestine intelligence activities. Similar provisions exist in the Right to Financial Privacy Act and the Fair Credit Reporting Act.[349]

[336] Hoofnagle, p. 620; See also Center For Democracy & Technology, available at: http://www.cdt.org/security/usapatriot/030528cdt.pdf.
[337] Doyle, p. 1; Bignami, p. 16.
[338] Bignami, p. 16, referring to the cases *Doe v. Ashcroft*, 334 F. Supp. 2d 471, 484-85 (S.D.N.Y. 2004) *(minimal requirements)*; *United States v. Molton Salt Co*., 338 U.S. 632 (1950); *Doe v. Ashcroft*, 334 F. Supp. 2d 471, 484-85 (S.D.N.Y. 2004) *(purpose).*
[339] 18 U.S.C. § 2510, 18 U.S.C. § 2518, 18 U.S.C. § 2703, 18 U.S.C. § 3123.
[340] 18 U.S.C. Chapters 119 (18 U.S.C. 2510 et seq.), 121 (18. U.S.C. 2701 et seq.) and 206 (18 U.S.C. 3121 et seq).
[341] 18 U.S.C. § 2518(3).
[342] 18 U.S.C. § 2701(c)(3); See also Kerr, 72 Geo. Wash. L. Rev. 1208, p. 1213.
[343] 18 U.S.C. § 2703(a), (b) and (c).
[344] Bignami, p. 21.
[345] 18 U.S.C. § 2518; 18 U.S.C. § 2703; 18 U.S.C. § 3122 et seq.
[346] 18 U.S.C. § 2518 (5).
[347] 18 U.S.C. § 2518 (8) (d); 18 U.S.C. § 2703 (b).
[348] 18 U.S.C. § 2705.
[349] 12 U.S.C. § 3414(a)(2) [access to financial records], 15. U.S.C. § 1681u [consumer records], 15. U.S.C. § 1681v(a) [consumer reports].

However, such requests can not be carried out, if the suspicious person is a US citizen and the investigation is solely based on activities protected by the First Amendment to the Constitution.[350]

The FBI can prohibit the service provider from informing any other person of the request (the so called "**gag rule**"), with the exception of an attorney to obtain legal advice.[351] The requirement of nondisclosure is subject to **judicial review**.[352] This section was subject to recent changes by the **FREEDOM Act**, which introduced, amongst others, some criteria for the application of the nondisclosure requirement. It should apply in cases when a senior official of the FBI certifies that the absence of such prohibition of disclosure may results in (i) a danger to the national security of the United States; (ii) interference with a criminal, counterterrorism, or counterintelligence investigation; (iii) interference with diplomatic relations; or (iv) danger to the life or physical safety of any person.[353]

Further, the FBI can distribute the information obtained to other parties, if this is provided for in specific guidelines or if "such information is clearly relevant to the authorized responsibilities of such agency".[354] Further changes through the **FREEDOM Act** specify the conditions for the FBI's access to the requested information by introducing the requirement that the request must use "a term that **specifically identifies a person, entity, telephone number, or account as the basis for a request**".[355] Similar changes have been made with regard to the access conditions to financial and consumer records, as well as consumer reports.[356] These more tailored request conditions should prevent bulk data collection.

In addition, **remedies** in the form of criminal penalties, as well as civil damages in cases of misuse, are available.[357] Violations can also lead to the exclusion of the illegally obtained information from evidence.[358] However, restrictions on **further use** of the collected data are not stipulated. For instance, data collected in the framework of the Wiretap Act can be used for LE, foreign intelligence and national security purposes.[359] The mentioned guarantees of the ECPA apply equally to all persons concerned, **independent of their nationality**.[360] However, with regard to NSL requests concerning investigations in the framework of the first amendment to the Constitution, the Stored Communication Act makes a distinction between US and non-US persons.

In summary, the data protection framework in an ordinary criminal investigation context is limited, but not completely nonexistent. However, as there is no general data protection framework for the private sector, the sector specific guarantees contained in the different Acts make it difficult to come to general conclusions. Additionally, the aforementioned third party doctrine hinders effective protection if data are handed over to private parties in the framework of contractual relations and then subsequently accessed by LE.[361]

[350] 18 U.S.C. § 2709(b).
[351] 18 U.S.C. § 2709(c).
[352] 18 U.S.C. § 3511.
[353] 18 U.S.C. § 2709(c).
[354] 18 U.S.C. § 2709(e).
[355] 18 U.S.C. § 2709(b).
[356] Compare Section 501 of the Freedom Act.
[357] 18 U.S.C. § 2520; 18 U.S.C. § 2707 and § 2712; 18 U.S.C. § 3121(d).
[358] Wiretap Act: 18 U.S.C. § 2518(10)(a); there is no such provision in the Stored Communications Act or the Pen Register Act.
[359] 18 U.S.C. § 2517; 18 U.S.C. § 2707.
[360] Bignami, p. 19, referring to the case *Suzlon Enegrgy Ltd. v. Microsoft Corp*., 671 F. 3d 726, 729 (9th Cir. 2011).
[361] Compare section 3.1.

3.4.2. National Security Investigations in PATRIOT, FISA and FREEDOM Act

In addition to the ordinary criminal investigations, an important part of US data collection takes place within the framework of national security inquiries. The main instruments used by investigating authorities are provisions contained in the **PATRIOT Act** and the **FISA**. In particular, the PATRIOT Act strengthened LE investigatory tools with regards to national security investigations. The Act made numerous amendments to existing statutory law, including FISA and ECPA. Many of the temporary provisions of the PATRIOT Act have been reauthorized several times, *inter alia* by the USA PATRIOT Improvement and Reauthorization Act of 2005, and the PATRIOT Sunset Extension Act of 2011.[362]

The FISA originally only provided a framework for the "electronic surveillance" of foreign intelligence information in the interest of national security (the so-called "traditional FISA orders").[363] Through the amendments of *inter alia* the PATRIOT Act and the FISA Amendments Act of 2008 (FAA), the scope of application of the existing FISA instruments has been broadened and additional instruments have been added.

Today's most important FISA instruments are included in **Chapter 36 of Title 50 of the U.S. Code**. They consist of: (i) a provision added by **Section 215 of the PATRIOT Act**, which allows the access to certain business records for foreign intelligence and international terrorism investigations (non-content information under the notion of "tangible things", **50 U.S.C. § 1861**), (ii) the metadata surveillance (**50 U.S.C. § 1842**) and (iii) an instrument added by the FAA which authorizes the government to collect foreign intelligence information of any type (also content information) on any non-US person reasonably believed to be located outside the United States (**50 U.S.C. § 1881(a) = Section 702 PATRIOT Act**).[364] The whole Chapter 36 distinguishes between US persons and non-US persons.[365]

Most recently, the **FREEDOM Act** restored, renewed and modified the mentioned provisions of the FISA and the PATRIOT Act, which had expired the day before. With the exception of the FREEDOM Act, all of the above mentioned provisions are discussed in the *Bignami* study in detail. The current analysis therefore **focuses on the changes made by the FREEDOM Act**.

3.4.2.1. Changes by the FREEDOM Act with regard to the collection of any tangible things for foreign intelligence purposes

The provisions of 50 U.S.C. Chapter 36, subchapter IV regulate the access to certain business records for foreign intelligence purposes and international terrorism investigations. It is based on **Section 215 of the PATRIOT Act** and mainly regulated in 50 U.S.C. § 1861 and § 1862. These provisions authorize *inter alia* the bulk collection of phone records and were modified after reaching their expiration date on June 1, 2015. The following analysis will also be a starting point for the presentation of very similar modifications of other measures provided for in Chapter 36, which were conducted by the FREEDOM Act.

The rules of subchapter IV generally empower the FBI to access certain business records and **any tangible things** in connection with an LE investigation activity, that is within the framework of 50 U.S.C. § 1861(a)(2). The request for access must aim at obtaining foreign intelligence information not concerning a US person or protecting against international

[362] Compare section 3.4.
[363] 50 U.S.C. §§ 1804, 1805.
[364] 50 U.S.C. § 1881(a).
[365] 50 U.S.C. § 1801(i).

terrorism or clandestine intelligence activities.[366] The obtained information on non-US persons can be shared with others for any lawful purpose.[367]

A necessary prerequisite to collect the information is the approval of a judge. Only if the judicial authority finds that the application made by the FBI meets the necessary requirements, business records can be accessed.[368] The application by the FBI can be made to a judge of the FISA Court or a designated US Magistrate Judge.[369] To be successful the application must have a specific content, which is described in 50 U.S.C. § 1861(b)(2). With regard to this content, the enactment of the FREEDOM Act has led to considerable changes which also affect data protection standards.

Specific selection term

According to the former version of 50 U.S.C. § 1861, the application for a collection order had to contain a statement of facts that proves there are reasonable grounds to believe that the tangible things sought are relevant for an authorized investigation and an enumeration of minimization procedures adopted by the Attorney General.[370] The FREEDOM Act introduces a different structure and new conditions with regard to the content of a search order by adding two more subparagraphs. The first modification (subparagraph (A)) requires a "**specific selection term** to be used as the basis for the production of the tangible things sought."[371] The second modification is the introduction of an independent procedure for the collection of call detail records on an ongoing basis in subparagraph (C).[372] This new subparagraph specifies the content of the statement of facts, if **call detail records** shall be provided to the FBI **on an ongoing basis**. Similar to the new subparagraph (A), the FBI is obliged to present a "specific selection term" in those cases. If the FBI wants to acquire **any other tangible things** the procedure in subparagraph (B) – which was subparagraph (A) before the introduction of the new subparagraphs – must be followed in addition to meeting the requirements of the new subparagraph (A). So in all cases, a **specific selection term** must be presented by the FBI in its application for a search order. This condition applies regardless of the citizenship and aims at preventing bulk collection of data within the US. To increase the clarity of these provisions the FREEDOM Act gives a definition of this newly introduced term.[373] Basically, a specific selection term means a term that specifically identifies a person, account, personal device, address or any other specific identifier.[374]

[366] 50 U.S.C. § 1861(a)(1).
[367] 50 U.S.C. § 1861(h).
[368] 50 U.S.C. § 1861(c)(1).
[369] 50 U.S.C. § 1861(b)(1).
[370] 50 U.S.C. § 1861(b)(2)(A) and (B).
[371] Section 103(a) of the Freedom Act.
[372] Section 101(a)(3) of the Freedom Act.
[373] Section 107 of the Freedom Act.
[374] Section 107 of the Freedom Act.

Emergency authority

A new subsection added by the FREEDOM Act at the end of subchapter IV raises some concerns.[375] Under certain circumstances companies have to provide the requested information without prior approval by a judge. The emergency authority of the Attorney General is an exception to the rule that a decision by an independent court has to be made before the FBI can access the information. However, a judicial control *ex-post* is required. The Attorney General has to apply for a judicial order within seven days after the request for access has been made.[376] To protect individuals from misuse the information acquired may generally not be used as evidence, if the application by the Attorney General was denied.[377] The information is further not allowed to be subsequently used or disclosed without the consent of the person concerned. The latter restriction, however, only applies to US persons.[378]

Time limit and erasure

The judicial approval constitutes the legal basis for the request of the FBI. Its content must fulfill specific requirements which are laid down in 50 U.S.C. § 1861(c)(2). The FREEDOM Act made additional requirements with regard to the request for call detail records. The court order authorizing the production of call detail records on a daily basis must not exceed a period of 180 days.[379] Although an extension is possible under certain circumstances, this provision shows that the legislator declines the idea of indefinite data collection with regard to call detail records. The time limit is supposed to protect the rights of individuals better.

Moreover, a further safeguard is implemented when it regards the access to call detail records. In its order, the court shall direct the governmental authority to adopt minimization procedures that require the prompt destruction of records, if it is determined that they do not contain foreign intelligence information.[380] The destruction of records shall also take place, if the minimization procedures themselves require this.[381] The introduced obligation for the FBI to erase records under certain conditions is an improvement compared to the former provisions. However, this progress is practically limited to US persons, since their call detail records can not regularly be qualified as foreign intelligence information, which is exempted from the erasure provision.

Judicial Control and minimization procedures

As already stated above, the application for a collection order by the FBI must contain an enumeration of the minimization procedures.[382] The FREEDOM Act strengthens the importance of this instrument. It introduces a new wording in 50 U.S.C. § 1861(c)(1). The application may only be accepted and the order may only be subsequently issued by the judge, if he/she, in addition to the already existing conditions, is satisfied that the minimization procedures submitted fall within the scope of the legal definition.[383] The

[375] Section 102 of the Freedom Act.
[376] Section 102(i)(3) of the Freedom Act.
[377] Section 102(i)(5) of the Freedom Act.
[378] Section 102(i)(5) of the Freedom Act.
[379] Section 101(b)(3) of the Freedom Act.
[380] Section 101(b)(3)(F)(vii) of the Freedom Act.
[381] Section 101(b)(3)(F)(vii) of the Freedom Act.
[382] 50 U.S.C § 1861(b)(2)(D) (new) according to Section 101(a)(2) of the Freedom Act.
[383] Section 104(a)(1) of the Freedom Act.

definition can be found in § 1861(g).[384] However, this definition relates only to information collected on US persons.

Besides this, the court also has the authority to impose additional, particularized minimization procedures.[385] These additional procedures may, in the interest of data subjects, require the destruction of information within a reasonable time period and regulate the production, retention or dissemination of the collected information.[386] Again, these additional protection measured are restricted to (unconsenting) US persons.

Beyond the implementation of minimization procedures, the FREEDOM Act introduces a structural modification with regard to the judicial control through the FISA Court. At the end of § 1803 a new subsection is added providing for the appointment of an "amicus curiae" to better consider the expertise of third parties in FISA decisions.[387] Individuals serving as an amicus curiae should be *inter alia* "persons who possess expertise in privacy and civil liberties [and] intelligence collection".[388] Further, the judicial review of FISA nondisclosure or production orders is now explicitly mentioned in 50 U.S.C. § 1861(f)(2).

Supervision and transparency

Some additional changes are made with regards to the improvement of transparency and supervision of the data collection procedures in the framework of the FISA and the PATRIOT Act. Section 108 of the FREEDOM Act amends the Section 106A of the USA PATRIOT Improvement and Reauthorization Act of 2005, which includes the regulation of the auditing process and accessing of certain business records for foreign intelligence purposes. Audit procedures shall now contain the years 2012-2014 and it should be verified whether the minimization procedures "adequately protect the constitutional rights" of US persons.[389] Further, the importance of the information acquired under title V of the FISA should be assessed, including the manner in which such information was collected, retained, analyzed and disseminated by the intelligence community.[390]

In addition, the Attorney General shall conduct a "declassification review of each decision, order or opinion issued by the FISA or the FISA review court" that includes a significant construction or interpretation of any provisions of law, including the interpretation of the newly introduced term "specific selection term".[391] Exceptions from the declassification requirement exist, if they are necessary to protect the national security of the US. Furthermore, the publication of the results in a redacted form is also possible.[392]

Additional FISA transparency and reporting requirements towards the Congress are stipulated in the renewed § 50 U.S.C. § 1862. These reporting duties include all compliance

[384] 50 U.S.C. § 1861(g) reads as follows: In this section, the term "minimization procedures" means — (A) specific procedures that are reasonably designed in light of the purpose and technique of an order for the production of tangible things, to minimize the retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information; (B) procedures that require that nonpublicly available information, which is not foreign intelligence information, as defined in section 1801(e)(1) of this title, shall not be disseminated in a manner that identifies any United States person, without such person's consent, unless such person's identity is necessary to understand foreign intelligence information or assess its importance; and (C) notwithstanding subparagraphs (A) and (B), procedures that allow for the retention and dissemination of information that is evidence of a crime which has been, is being, or is about to be committed and that is to be retained or disseminated for law enforcement purposes.
[385] Section 104(a)(3) of the Freedom Act.
[386] Section 104(a)(3) of the Freedom Act.
[387] Section 401(i) of the Freedom Act.
[388] Section 401(i)(3) of the Freedom Act.
[389] Section 108(1) of the Freedom Act.
[390] Section 108(1) of the Freedom Act.
[391] Section 602(a) of the Freedom Act.
[392] 50 U.S.C. § 1862 (new) according to Section 602(a) of the Freedom Act.

reviews conducted by the government for the production of tangible things, the total number of applications made for orders approving requests for the production of tangible things, the total number of such orders either granted, modified or denied and also the total number of applications made for orders in which the specific selection term does not specifically identify an individual account or personal device.[393] Further, companies subject to nondisclosure requirements may publish a semiannual transparency report showing the number of orders, directives or NSLs received, reported in bands of 1000.[394]

Transition period

As stated in Section 109(a), the provisions from Sections 101 to 103 (on tangible things) of the FREEDOM Act are subject to a transition period. The current provisions will ultimately expire on November 29, 2015. The existing bulk data collection will therefore continue until the end of November 2015.[395]

3.4.2.2. Changes made through the FREEDOM Act with regard to metadata surveillance

Subchapter III of Chapter 36 regulates the interception of metadata through the use of pen registers and trap-and-trace devices for foreign intelligence and international terrorism investigations.[396] The orders in this chapter authorize the capturing of information about source, destination, time and date of electronic communications, but not their content.[397] Pen registers are devices or processes recording outgoing wire or electronic information of telephone or internet communication, while trap-and-trace devices capture incoming information.[398] Upon governmental request, a communication provider or any other person is obliged to install and operate these devices while at the same time being obliged to not disclose the existence of the investigation.[399] The information obtained by LE can then be disclosed for any lawful purpose.[400]

While the existing conditions for issuing a metadata surveillance order remain unchanged, the FREEDOM Act introduces an additional criterion to be respected by the government when applying for a surveillance order. As mentioned above in the framework for the collection of any tangible things (including call detail records), a **specific selection term** must also be used in this context to identify a person, account, address, or personal device.[401] Broad geographic areas, for instance, are prohibited from serving as selection terms.[402] The term should be "used to limit to the greatest extent reasonably practicable, the scope of information sought, consistent with the purpose of seeking the use of the pen register or trap and trace devices" and applies to all searches within the US regardless of the citizenship.[403] The purpose of the investigation remains the same and is focused on obtaining foreign intelligence information (if a non-US person is targeted) or to protect against international terrorism or clandestine intelligence activities, provided that such an

[393] 50 U.S.C. § 1862 (new) according to section 601 of the Freedom Act.
[394] Section 604 of the Freedom Act.
[395] Compare primary order issued on 27 August 2015 by the US Foreign Intelligence Surveillance Court, Nr. BR15-99, approved for public release as redacted by the ODNI 20150828, available at: http://www.justice.gov/opa/pr/joint-statement-department-justice-and-office-director-national-intelligence-declassificati-1.
[396] 50 U.S.C. §§ 1841 et seq.
[397] See definitions of "pen register" and "trap and trace device" 50 U.S.C. § 1841(2), 18 U.S.C. § 3127(3) and (4).
[398] 50 U.S.C. §1841(2), 18 U.S.C. §3127(3) and (4); Wong, p. 241.
[399] See in details 50 U.S.C. §1842(d)(2)(B).
[400] 50 U.S.C. § 1845.
[401] 50 U.S.C. § 1842(c)(3) (new), introduced trough Section 201 of the Freedom Act.
[402] 50 U.S.C. § 1841(4)(A).
[403] 50 U.S.C. § 1841(4)(A).

investigation into a US person is not based on activities protected by the First Amendment.[404] The FISA Court is in charge of verifying these requirements.[405]

In addition, the FREEDOM Act introduces so called "**privacy procedures**" meaning that the Attorney General should ensure "that appropriate policies and procedures are in place to safeguard nonpublicly available information" that is collected by the devices and which concern US persons.[406] There is no further definition of privacy procedures or the meaning of appropriate policies that are in place and, as usual, these procedures relate solely to US persons. Moreover, the FISA Court and the Attorney General are empowered to impose additional privacy or minimization procedures.[407]

3.4.2.3. Changes made through the FREEDOM Act with regard to information on persons outside the US

Subchapter VI of Chapter 36 concerns the collection of information of non-US citizens on foreign soil.[408] It was introduced through **Section 702 of the FISA Amendment Act** of 2008 and entails procedures for targeting persons outside the US. It is one of the most disputed provisions of FISA as it represents the legal basis for mass surveillance of non-US communication and NSA interception programs such as PRISM.[409] In particular, 50 U.S.C. § 1881(a) authorizes far-reaching surveillance of foreign intelligence information, including communications, content, metadata or records. Although this subchapter has continually been and still is subject to heavy criticism, the FREEDOM Act did not make any major changes regarding this subchapter. The only considerable change concerns the exclusion of evidence of illegally obtained information on US persons during surveillance. Without consent, such information cannot be used as evidence, an exception is made when the FISA Court permits the use.[410] The general rules regarding traditional electronic surveillance on minimization procedures or disclosure for lawful purposes apply to this section.[411] With reference to the amendments through the FREEDOM Act, it is worth noting that the surveillance does not need to relate to a specific term individualizing the targeted non-US person, as is necessary with regards to US persons in the other cases described above. The current regulatory framework of this section clearly contradicts EU data protection law and a clarification with regard to the collection possibilities of this section in future negotiations with the US is recommended.

US criticism stems from the fact that by collecting the traffic abroad, authorities can presume that the traffic belongs to foreigners. Any US person's traffic that happens to be captured during a bulk collection is considered "incidentally collected" and may therefore be retained for further processing.[412]

3.4.3. Elements remaining unchanged by the FREEDOM Act

Primarily, the FREEDOM Act intends to improve the protection of US persons in the framework of data collection by LE and intelligence agencies. Therefore, the Act does not include major changes with regards to the protection of non-US persons in this context. Instruments such as **Executive Order 12333**, whose main focus is to regulate human and

[404] 50 U.S.C. §1842(a)(1).
[405] 50 U.S.C. §1842(b).
[406] Section 202 codified in 50 U.S.C. § 1842(h)(1).
[407] Section 202 codified in 50 U.S.C. § 1842(h)(2).
[408] 50 U.S.C. § 1881 et seq.
[409] Bignami, p. 25.
[410] 50 U.S.C. § 1881a(i)(3).
[411] Compare 50 U.S.C. § 1881(e) referring to 50 U.S.C. § 1806.
[412] Arnbak/Goldberg, pp. 321 and 325.

technical collection techniques undertaken abroad, remain unchanged.[413] This order is applicable in "addition to and consistent with" existing laws and is therefore highly relevant for areas of surveillance not covered by FISA.[414] The collection of foreign intelligence is not restricted to a specific type of information[415] and incidentally obtained information can be shared with LE authorities, when it indicates involvement in activities that may violate federal, state, local or foreign laws.[416]

In addition, the order entails fewer guarantees for individuals when compared to the FISA provisions mentioned above. [417] For instance, oversight is not carried out by a court or any other judicial body, but through internal mechanisms inside the intelligence community.[418] As most of the FISA provisions, any existing limitations on foreign intelligence surveillance are primarily designed to protect US persons.[419] Intelligence agencies are, for instance, authorized to collect, retain and disseminate information on US persons only in accordance with procedures set down under departmental guidelines and which are approved by the Attorney General.[420] Thereby the agencies shall use the least intrusive collection techniques feasible within the US or directed against US persons abroad.[421] The mentioned restrictions regarding the permitted collection methods only apply to US persons.

A further instrument that has not been included in the FREEDOM Act is the Presidential Policy Directive 28, which was seen as a major improvement concerning data protection guarantees for non-US persons.[422] This Directive was issued in January 2014 and included some restrictions on bulk data collection, proportionality elements and certain privacy protections for individuals concerned in the context of data collection of non-US persons.[423] However, these ideas, which were regarded as a "conceptual shift" in US policy[424], are not mirrored in the FREEDOM Act.

Furthermore, no considerable changes are made with regard to **traditional FISA orders** for electronic surveillance in the framework subchapter 1 of Chapter 36.[425] Two smaller changes regard the extension of the definition of "agent of foreign power", which now refers to persons independent of their actual presence inside or outside US territory[426], and a newly introduced 72 hour time limit for the continued surveillance of non-US persons, who were previously believed to be outside the US, but who entered the US territory when the surveillance measure was already in place.[427]

3.5. Key Findings

Clearly, the structural differences, between rights and procedures applying to US persons and non-US persons, which are evident when data protection guarantees in LE and national security investigations are analyzed, is a major concern. The rights applying to US persons

[413] See § 2.2 of Executive Order 12333.
[414] §§ 2.2 and 2.5 Executive Order 12333 and Bignami, p. 27.
[415] Definition of "foreign intelligence" in § 3.5 (e) Executive Order 12333.
[416] § 2.3 (i) Executive Order 12333.
[417] Arnbak/Goldberg, p. 338.
[418] § 1.6 (b), (c) and (h) Executive Order 12333.
[419] Bignami, p. 27.
[420] § 2.3 Executive Order 12333.
[421] § 2.4 Executive Order 12333.
[422] The White House, Presidential Policy Directive – Signals Intelligence Activities, available at: https://www.whitehouse.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities.
[423]Compare for details, Bignami, pp. 28 et seq.
[424] Bignami, pp. 28 et seq.
[425] 50 U.S.C. §§ 1801 et seq; for more details on traditional FISA orders, compare Bignami, pp. 22 et seq.
[426] Section 702 codified in Note on 50 U.S.C. § 1801.
[427] Section 701(a)(2) codified in 50 U.S.C. § 1805(f).

already lack a general data protection framework; this weakness is intensified when non-US persons are concerned. While in ordinary criminal investigations, limited, but equal, rights for the persons concerned exist, investigations concerning national security highlight the structural divide. The proposed laws, such as the Draft Judicial Redress Act and the FREEDOM Act, intend to rudimentarily remedy this shortcoming, but fail in granting equal or at least similar rights to non-US persons. The Draft Judicial Redress Act is limited in scope as it only encompasses "covered records", which are records transferred from an EU authority or private entity to a US authority covered by the Draft Bill for the purpose of preventing, investigating, detecting or prosecuting criminal offences. Records obtained or collected by other means, in other contexts or by authorities not covered by the Act, are therefore not protected. Consequently, the mass data collection criticized in the context of national security investigations will almost certainly not be regulated by the Act. Further, only three out of four remedies of the Privacy Act are available to covered persons according to the Draft Judicial Review Act leaving the individual with no judicial review possibilities in case that an agency fails to provide for an accurate, relevant, timely and complete treatment of the individual's data.

The newly introduced FREEDOM Act changes some provisions in the framework of national security investigations, but otherwise reinforces the structural divide between US and non-US persons. As its primary goal is a reinforced protection of US citizens in the framework of LE and foreign intelligence collection, most of the changes concern improvements for US persons. Measures such as minimization procedures, improved rights with regards to the destruction of records, audit requirements or so called "privacy procedures" exclusively concern US persons.

Nevertheless, the introduction of a specific selection term for the collection of tangible things and metadata for foreign intelligence purposes is clearly seen as progress compared to the former regulation. However, this instrument (the specific selection term) is not used in the framework of Section 702 of the FISA Amendment Act (in particular 50 U.S.C. § 1881 (a)), which authorizes far-reaching surveillance of foreign intelligence information, including communications, content, metadata or other records. Moreover, the FREEDOM Act does not change traditional FISA orders or the Executive Order 12333.

4. SUMMARIZING COMPARISON

Comparing EU and the US data protection legislation for LE purposes is a difficult task due to the fundamental structural, constitutional and practical legal differences visible in the prior analysis. A summarizing comparison can therefore only refer to and identify the most striking differences and shortcomings, with the details being elucidated in the comprehensive analysis above.

The most prominent and important divergence concerns the constitutional protection of personal data. While data protection and privacy are fundamental rights in the EU and are also applicable in the LE context, there is no equivalent protection in the US. The EU's understanding of these rights have been shaped since the 1970s by comprehensive case law of the ECtHR and was been further developed in recent years through important EU instruments such as the Directive 95/46/EC, the TFEU and the Charter of Fundamental Rights, as well as the EU courts' case law. The US, with its restrictions to the protection of the Fourth Amendment, through the Third Party Doctrine, and the exclusion of non-US persons from both the Fourth Amendment and the Privacy Act protection, follow a very different approach, which is contrary to the EU's perspective of privacy and data protection as comprehensive fundamental rights.

The EU data protection canon consists of several principles, which mainly apply independently of the context. They include, amongst others, rules on data quality standards, on sensitive data, independent supervision, the purpose limitation principle, rules on inter-agency exchange or transfer of data to third states, time limits for the retention of data, effective judicial review and access possibilities, independent oversight, proportionality elements, notification requirements after surveillance or data breaches, access, correction and deletion rights as well as rules on automated decisions, data security as well as technical protection. These rights and principles are subject to restrictions, but these restrictions are limited by proportionality elements and are continually subject to judicial review. Some of the mentioned EU rights, such as notification, supervision or judicial review can also be found in certain US Acts, for instance in the ECPA. However, they only exist in a mitigated form and are often subject to far-reaching restrictions, when LE or national security interests are concerned. These restrictions are not limited by proportionality considerations, leading to a structural and regular prevalence of LE and national security interests.

While some legal concepts are similar to a certain extent, most of the EU data protection guarantees simply do not exist in US law. One example illustrating a certain degree of similarity is supervision. While the idea of oversight and supervision can be found in both jurisdictions, supervision according to EU rules must be independent of the supervised agency, whereas internal supervisory mechanisms dominate the US LE and national security sector. Other basic EU data protection principles such as restrictions on the further use and dissemination of data collected in an LE context, purpose limitation, or time limits on data retention do not exist at all or only rudimentarily exist in the US. In particular, the approach to data sharing is fundamentally different. Whilst under EU law every transfer of data to other agencies interferes with fundamental rights and requires specific justification, largely unrestricted data sharing between LE authorities and the intelligence community in the US seems to be the rule, rather than the exception.

A further crucial distinction is the approach taken to determining the scope of a law protecting privacy and data protection of individuals. While privacy restrictions in the EU are usually considered in a balancing of interests, focusing on proportionality requirements, US laws often restrict the scope of application of the law itself, thereby considerably

limiting its scope from the outset. An example is the Draft Judicial Redress Act, whose application is limited to "covered records" and "covered countries".

Moreover, while in the EU, the existence of a legal act interfering in general with fundamental rights is sufficient to trigger a standing for the individual to sue, the existence of bulk collection of data in the US does not automatically lead to an individual right of action. In the recent *Klayman* case, the US Court of Appeals for the District of Columbia Circuit stated that *Klayman* has no standing to sue as the plaintiffs "lack[s] direct evidence that records involving their calls have actually been collected."[428] The possibility of judicial review in light of this ruling consequently appears to be limited.

Another important difference relates to the protected persons. Whereas in EU law, fundamental rights cover all persons targeted by LE and surveillance measures, regardless of their nationality or domicile, US law distinguishes between US and non-US persons and discriminates against the latter. This distinction is clearly visible in the provisions regulating foreign intelligence surveillance, such as the FISA and the PATRIOT Act. Newly introduced laws, such as the FREEDOM Act, do not remedy or change this situation. Only with regards to ordinary criminal investigations, the same rights apply to US persons as to non-US persons.

However, the introduction of stricter access conditions for the collection of tangible things and metadata for foreign intelligence purposes through the newly introduced criterion of the specific selection term in the FREEDOM Act is an improvement compared to the previous predominantly unregulated bulk data collection. Its intention is to limit mass data collection by introducing more restrictive criteria to identify a specific person, entity or account during surveillance. Governmental authorities must now prove that they search for a specific individual or account in order to obtain a FISA order in order to access metadata, call detail records or other tangible things. Regrettably, this newly introduced restriction does not concern Section 702 of the FISA Amendment Act, which authorizes far-reaching surveillance of foreign intelligence information, including communications, content, metadata or other records. This (mass) access to content would clearly violate EU fundamental rights (cf. data retention case and opinion of Advocate General *Bot* in the *Schrems* case).

With regards to existing EU-US data sharing agreements such as the Safe Harbor regime, it can be concluded that this instrument is not applicable to current data protection standards anymore and clearly needs to be adapted to overcome the existing shortcomings. This view was very recently confirmed by the opinion of Advocate General *Bot* in the *Schrems* case.[429]

From the analysis above, it can be deduced that even if all existing data protection guarantees applying to US persons in the LE and national security framework were made applicable to EU citizens, there would be a considerable difference regarding the level of privacy and personal data protection. The newly introduced Judicial Redress Act and the FREEDOM Act only partially improve this rather unsatisfying situation.

[428] United States Court of Appeals, District of Columbia Circuit, *Klayman v. Obama*, no. 14-5004, consolidated with nos. 14-5005, 14-5016, 14-5017, decided 28 August 2015, available at: https://assets.documentcloud.org/documents/2301510/read-the-dc-circuit-court-ruling-against-the-nsa.pdf

[429] CJEU, C-362/14 *Schrems*, opinion of 23rd of September, available at: http://curia.europa.eu/juris/document/document.jsf?text=&docid=168421&pageIndex=0&doclang=en&mode=req&dir=&occ=first&part=1&cid=518391.

5. CONCLUSIONS AND POLICY RECOMMENDATIONS

This comparative study between EU and US data protection guarantees in the field of law enforcement has illustrated important differences in the legal and constitutional protection of personal data. These discrepancies make it difficult to carry out a comparison, as the protection mechanisms already vary fundamentally from their very outset. As a general finding, it can be established that whilst the EU data protection framework in the LE sector is shaped by comprehensive data protection guarantees, which are codified in EU primary and secondary law accompanied by EU and ECtHR case law, the US data protection guarantees in the LE and national security sector vary according to the instruments in place and are far less comprehensive. In particular, constitutional protection is limited, even with regards to US citizens and when data protection guarantees do exist in federal law; furthermore they usually do not include protection for non-US persons. In the US proportionality considerations do not play a decisive role in the determination of restrictions to data protection rights of individuals, thus LE and national security interests typically prevail over the interests of the individual concerned.

A majority of the EU data protection standards cannot be found in US law. A comparison is therefore not possible. Rules limiting inter-agency data exchange, exchange with other third parties, complete independent oversight and effective judicial review possibilities for non-US persons simply do not exist at all or are at best very limited. These shortcomings are further visible in existing data exchange agreements, such as the Safe Harbor regime. Policy recommendations therefore refer to a future regulation of LE data exchange between the EU and the US. They can be summarized as follows:

- A future "Umbrella Agreement" must not only concentrate on procedural elements by guaranteeing effective judicial review for EU citizens, but should also focus on the other mentioned material data protection guarantees that build the basis for a comprehensive protection framework within the EU. Independent supervision, the regulation of onward transfer, the inter-agency data exchange within the US, the application of minimization procedures also for EU citizens, notification requirements after surveillance or data breaches, access, correction and deletion rights, and a limitation of the purpose of a data transfer, are essential elements in this context.

- The proposed Judicial Redress Act will not solve the structural imbalance between the protection of US and non-US persons. The Draft Act has a limited scope, referring only to "covered records". This notion and the concrete application of the rights entailed in this Act should be clarified. If it only relates to data transferred from EU agencies or private entities in an LE context, it is possible that it excludes all other forms of data access via, for instance, the access in the framework of national security, which is still been carried out and subject to harsh criticism. In addition, the Draft Act only refers to certain rights to sue for covered persons, while excluding others, in particular 5 U.S.C. § 552a(g)(1)(d) of the Privacy Act. Therefore, the Judicial Redress Act does not necessarily guarantee equal rights to EU and US persons. However, the question of equal treatment is essential in future data exchange agreements.

- A further indispensable point concerns the still ongoing collection of foreign intelligence in the framework of Section 702 of the FISA Amendment Act and Executive Order 12333. The FREEDOM Act did not bring about any major changes regarding these instruments with regards to the protection of EU citizens. A future instrument regulating data exchange should address these two issues, as serious

questions on their compatibility with EU fundamental rights arise (see recent opinion of Advocate General *Bot* in the *Schrems* case).

6. ADDENDUM: BRIEF ANALYSIS OF THE UMBRELLA AGREEMENT

The initial text of this study was finalized before the Umbrella Agreement had been published. At the request of the relevant European Parliament's services (Policy Department C and LIBE secretariat), the following remarks on this agreement were added after the Umbrella Agreement was leaked and subsequently published on the 15th of September, 2015.[430] The analysis gives an initial overview of the strengths and weaknesses of the agreement, but can only reflect a first impression. In addition, as the Commission has so far decided not to publish the text of the agreement via official channels, the subsequent remarks are based on the leaked version of the agreement.

In total, the agreement includes 29 Articles, which address at a first view many of the critical points discussed in this study. Above all, the agreement refers to judicial redress procedures for EU citizens and contains references to essential data protection guarantees, which are thus far only clearly stated in EU law, but not in US law. In the text substantial concessions from the US side are included, but upon a closer look at the provisions there is considerable leeway regarding the enforcement of some of these provisions and several other shortcomings which are briefly summarized hereinafter.

Judicial and administrative redress for EU citizens

The first, and perhaps the most important point, concerns the concession for the US to provide judicial redress procedures for EU citizens within the US. However, the agreement is far from being able to guarantee equal judicial redress rights to EU and US citizens. Instead of inserting a clause, simply making the guarantees of the US Privacy Act applicable to the individuals concerned, a complicated **two-step redress procedure** has been established.

In a first step, according to this redress procedure, an individual is "entitled to seek administrative redress where he or she believes that his or her request" for access, rectification or improper processing has been "improperly denied".[431] In a second step, and only after exhaustion of the administrative redress, an EU citizen (the agreement no longer uses the term individual anymore, but refers to a citizen, which **excludes data relating to non-EU citizens**) is granted the right to claim judicial redress. However, this **right is limited to three cases**. Only if a competent authority has been denied access to or after an amendment of records or if an unlawful disclosure of personal data has been "willfully or intentionally made" should judicial redress even be possible. Therefore, not all four causes of civil remedies mentioned in the Privacy Act are consequently available to EU citizens. Furthermore, remedies such as the general remedy under 5 U.S.C. § 552a(g)(1)(d) are narrowed down to wilful or intentional disclosures by the competent authorities.[432] There is hence no possibility for the individuals concerned to review the entire collection of data or the processing procedure as a whole. Moreover, the actual application of the procedure mentioned in the agreement depends on the adoption of the Judicial Redress Act, which is also subject to criticism.[433]

[430] See: http://statewatch.org/news/2015/sep/eu-us-umbrella-agreement-full-text.pdf.
[431] Article 18 (1) of the Umbrella Agreement in its leaked version of 15th September 2015.
[432] See also criticism above in section 3.3. and EPIC statement of 16th September 2015, available at: https://epic.org/foia/umbrellaagreement/EPIC-Statement-to-HJC-on-HR1428.pdf.
[433] See section 3.3.

Competent Authorities/Exclusion of national security

The scope of application of the mentioned remedies is further restricted to "Competent Authorities", referring to the LE authorities responsible for the prevention, investigation detection or prosecution of criminal offences, including terrorism.[434] The agreement thus **excludes data collected by national security authorities**.[435] The (mass) accessing of EU citizens data through such authorities in the framework of the FISA, PATRIOT or FREEDOM Act, as aforementioned[436], is thereby not covered by the guarantees of the agreement, meaning that, in practice, data originating from US national security agencies which are shared with LE authorities are not safeguarded by the agreement. In view of the common data-sharing activities between these agencies, the limitation of the agreement's scope in regards to data exchanged by LE authorities should be taken into account when judging its impact.

Oversight

The provisions regarding oversight are drafted in a somewhat **ambiguous** way. A clear obligation to implement independent oversight authorities is not included in the agreement. In its place, the US provides oversight "cumulatively" through a variety of different bodies, which does not correspond with the EU's understanding of independency.[437] Independent supervision is, nevertheless, the pre-requisite for an effective enforcement of individual rights. As recently discussed in the Advocate General's opinion in the *Schrems* case, existing US bodies, such as the FTC or private dispute resolution bodies which exercise supervision are restricted in their power and cannot be regarded as independent bodies under EU law.[438]

Enforcement of rights guaranteed

The parties of the agreement are obliged to "take all necessary measures to implement this Agreement".[439] The protections and remedies stated in the agreement must therefore be implemented in the respective domestic laws.[440] In practice, this would mean that the US would have to change their existing legislation to include privacy protection for EU citizens. Moreover, in some cases, in particular with regard to access, rectification and notification rights, as well as the protection of special categories of data and the limitation on automated data processing, implementation would necessitate the enactment of virtually completely new guarantees in US law. Whether such fundamental changes in US privacy legislation are actually intended in practice, is doubtful, considering the limited changes provided for in US law through the Draft Judicial Redress Act.

Notification

A welcomed provision, at least at a first glance, concerns the notifying of the transferring authority after an information security incident.[441] There are, however, **considerable exemptions** for this provision.[442] Moreover, contrary to EU regulations, notification is restricted to the LE authority transferring the data, information to the individual concerned

[434] Article 2 (5) of the Umbrella Agreement in its leaked version of 15th September 2015.
[435] Article 3 (2) of the Umbrella Agreement in its leaked version of 15th September 2015.
[436] Section 3.4.
[437] Article 21 (3) of the Umbrella Agreement in its leaked version of 15th September 2015.
[438] CJEU, Case C-362/14, *Schrems v. Data Protection Commissioner,* Opinion of the Advocate General Bot on 23rd of September 2015, para 204 et seq.
[439] Article 5 (1) of the Umbrella Agreement in its leaked version of 15th September 2015.
[440] Compare Articles 5 (2); 6 (5) (purpose and use limitations).
[441] Article 10 of the Umbrella Agreement in its leaked version of 15th September 2015.
[442] Article 10 (2) and (3) of the Umbrella Agreement in its leaked version of 15th September 2015.

or to the data protection authority supervising the transfer is not required, leaving a considerable leeway for LE authorities to forward this information to independent players, such as data protection authorities.

Onward transfer

The provisions on onward transfer to third states essentially correspond to the provisions in EU law by requiring the prior consent of the sending party for further transfer. However, the **US internal inter-agency exchange, which is fairly common and far-reaching, is not regulated** in detail by the agreement. There is a provision on "accountability" included in Article 14 of the Umbrella Agreement, but the wording of this article is rather vague and procedural rules concerning the enforcement of accountability are absent. The discontinuation of transfer to other domestic authorities is intended, as appropriate, if the other authority has "not effectively protected personal information", referring in particular to the purpose and use limitations and onward transfer provisions.[443] Which criteria actually play a role in the assessment of appropriateness or in the determination of effective protection remains unknown. The procedural rules on the control of accountability would certainly underpin the meaning of this provision.

Yet there is the possibility for the transferring authority to impose additional conditions for the transfer of data.[444] These additional conditions should "not include generic data protection conditions", which are conditions unrelated to the specific facts of the case.[445] While the exact meaning of this paragraph remains unclear, it can be assumed that data protection standards which go beyond the standards mentioned in the agreement will be difficult to practically implement.

Other remarks

The positive aspects of the agreement concern the inclusion of a non-discrimination clause, joint review procedures, the general mentioning of purpose and use limitations, access and rectification rights and the general possibility to impose additional conditions for transfer. Another important point relates to the obligation to lay down provisions on specific data retention periods in the respective domestic laws.[446] This would clearly necessitate changes in US legislation, as up to now fixed data retention periods with regards to LE data transferred from third countries do not exist.

Concluding comments

It is imperative to mention that the agreement has no effect on existing agreements and will therefore not resolve the situation with regards to current arrangements, such as the Safe Harbor regime. The Umbrella Agreement is consequently not a solution to the ongoing problem of (mass) access by US intelligence agencies to EU data.

Overall, one can deduce from the experience with the Safe Harbor agreement, that the exact wording of the agreement's provisions must be thoroughly considered, so as to avoid leaving a considerable leeway for a varied interpretation of vaguely drafted clauses, which would result in serious misunderstandings of the rights and duties included in the agreement.

[443] Article 14 (2) of the Umbrella Agreement in its leaked version of 15th September 2015.
[444] Article 6 (3) of the Umbrella Agreement in its leaked version of 15th September 2015.
[445] Article 6 (3) of the Umbrella Agreement in its leaked version of 15th September 2015.
[446] Article 12 of the Umbrella Agreement in its leaked version of 15th September 2015.

Finally, the overall impression of the agreement is ambiguous. It is clearly an important step in the right direction for an improved protection for individuals in the framework of transatlantic data transfer in the LE sector and a suitable starting point for the improvement of individual rights protection by restricting the mass circumvention of EU data protection laws. Despite the criticism mentioned above, the agreement entails some remarkable concessions from the US side; yet its exact meaning and practical implementation will have to be clarified in the upcoming legislative process.

LITERATURE REFERENCES

Arnbak A, Goldberg S (2015), Loopholes for Circumventing the Constitution: Unrestrained Bulk Surveillance on Americans by Collecting Network Traffic Abroad, 21 Mich. Telecomm. & Tech. L. Rev. 317, available at: http://repository.law.umich.edu/mttlr/vol21/iss2/3?utm_source=repository.law.umich.edu%2Fmttlr%2Fvol21%2Fiss2%2F3&utm_medium=PDF&utm_campaign=PDFCoverPages

Article 29 Data Protection Working Party, Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector, adopted on 27 February 2014, available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp211_en.pdf

Article 29 Data Protection Working Party, Opinion 15/2011 on the definition of consent, adopted on 13 July 2011, available at: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp187_en.pdf

Article 29 Working Party, WP 114 on a common interpretation of Article 26 (1) of Directive 95/46/EC, adopted on 25 November 2005, available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2005/wp114_en.pdf

Article 29 Working Party, WP 12 on the transfers of personal data to third countries: applying Articles 25 and 26 of the EU data protection directive, adopted on 24 July 1998, available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/1998/wp12_en.pdf

Article 29 Working Party, WP 9 on preliminary views on the use of contractual provisions in the context of transfers of personal data to third countries, adopted on 22 April 1998, available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/1998/wp9_en.pdf

Article 29 Working Party, WP 7 on the judging of industry self regulation: when does it make a meaningful contribution to the level of data protection in a third country?, adopted on 14 January 1998, available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/1998/wp7_en.pdf

Article 29 Working Party, WP 4 giving first orientations on the transfer of personal data to third countries – possible ways forward in assessing adequacy, adopted on 26 June 1997, available at: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/1997/wp4_en.pdf

Bignami F (2015), The US legal system on data protection in the field of law enforcement. Safeguards, rights and remedies for EU citizens, Study for the LIBE Committee, PE 519.215, available at: http://www.europarl.europa.eu/RegData/etudes/STUD/2015/519215/IPOL_STU%282015%29519215_EN.pdf

Boehm F (2011), European Flight Passenger Under General Suspicion – The Envisaged Model of Analysing Flight Passenger Data, published in: Privacy and Data Protection, An Element of Choice, S. Gutwirth/R. Leenes/P. de Hert/Y. Poullet (eds.), Springer, Chapter 8, pp. 171-191

Boehm F (2011), Information sharing and data protection in the Area of Freedom, Security and Justice – Towards harmonised data protection principles for EU-internal information exchange, Springer

Boehm F (2015), Legal opinion on the adequacy of the safe harbor decision, CJEU Case C-362/14 (opinion requested by the applicant), available at: http://www.europe-v-facebook.org/CJEU_boehm.pdf

Boehm F, Cole M (2014), Data retention after the Judgement of the Court of Justice of the European Union, available at: http://www.greens-efa.eu/data-retention-12640.html

Boehm F, de Hert P (2012), Notification, an important safeguard against the improper use of surveillance – finally recognized in case law and EU law, European Journal of Law and Technology, Vol. 3, No. 3, available at: http://ejlt.org/article/view/155/264

Boehm F, de Hert P (2012), The rights of notification after surveillance is over: ready for recognition?, Yearbook of the Digital Enlightenment Forum 2012, IOS Press, pp. 19-39

Boehme-Neßler V (2014), Das Recht auf Vergessenwerden – Ein neues Internet-Grundrecht im Europäischen Recht, NVwZ, pp. 825-830

Bowden C, Bigo D (2013), The US surveillance programmes and their impact on EU citizens' fundamental rights, Study for the LIBE Committee, PE 474.405, available at: http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/briefingnote_/briefingnote_en.pdf

Cannataci J A, Caruana M M (2013), Report: Recommendation R (87) 15 – Twenty-five years down the line, available at: http://www.statewatch.org/news/2013/oct/coe-report-data-privacy-in-the-police-sector.pdf

Center for Democracy & Technology (2003), Privacy's Gap: The Largely Non-Existent Legal Framework for Government Mining of Commercial Data, available at: https://www.cdt.org/files/security/usapatriot/030528cdt.pdf

Cole M, Boehm F (2014), EU Data Retention – Finally Abolished? CritQ, pp. 58-78

de Busser E (2009), Data Protection in EU and US Criminal Cooperation, Maklu Pub, pp. 103-105

Doyle C (2006), Administrative Subpoenas in Criminal Investigations: A Brief Analysis, Congressional Research Service, available at: https://www.fas.org/sgp/crs/intel/RL33321.pdf

European Data Protection Supervisor, Third opinion of the European Data Protection Supervisor on the Proposal for a Council Framework Decision on the protection of personal data processed in the framework of police and judicial co-operation in criminal matters, OJ 2007 C 139, 23.6.2007, pp. 1-10

European Data Protection Supervisor, Annex to Opinion 3/2015: Comparative table of GDPR texts with EDPS recommendations, available at: https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2015/15-07-27_GDPR_Recommendations_Annex_EN.pdf

Granger M-P, Irion C (2014), The Court of Justice and the Data Retention Directive in Digital Rights Ireland: Telling Off the EU Legislator and Teaching a Lesson in Privacy and Data Protection, European Law Review, Issue 6, pp. 834-850

Hoofnagle C J (2004), Big Brother's Little Helpers: How Choicepoint and other Commercial Data Brokers Collect and Package Your Data for Law Enforcement, 29 N.C. J. Int'l & Com. Reg, pp. 595-636

Kerr O S (2004), A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It, 72 Geo. Wash. L. Rev, pp. 1208-1250

Meyer-Ladewig J (2006), Europäische Menschenrechtskonvention, Handkommentar, 2nd edition, Nomos

Moreham N A (2008), The Right to Respect for Private Life in the European Convention on Human Rights: A Re-examination, European Human Rights Law Review, Issue 1, 2008, pp. 44-79

Ovey C, White R (2006), Jacobs&White - The European Convention on Human Rights, Fourth Edition, Oxford University Press

Peers S, Hervey T, Kenner J, Ward A (2014), The EU Charter of Fundamental Rights – A Commentary, C.H. Beck - Hart – Nomos

Siemen B (2006), Datenschutz als europäisches Grundrecht, Duncker & Humblot

Thompson R (2014), The Fourth Amendment Third-Party Doctrine, Congressional Research Service, available at: https://www.fas.org/sgp/crs/misc/R43586.pdf

Wong M W S (2002), Electronic Surveillance and Privacy in the United States after September 11, 2001: The USA-PATRIOT Act, Singapore Journal of Legal Studies, pp. 214-270

CAT: QA-02-15-743-EN-C (paper)
CAT: QA-02-15-743-EN-N (pdf)

DIRECTORATE-GENERAL FOR INTERNAL POLICIES

POLICY DEPARTMENT C
CITIZENS' RIGHTS AND CONSTITUTIONAL AFFAIRS

Role

Policy departments are research units that provide specialised advice to committees, inter-parliamentary delegations and other parliamentary bodies.

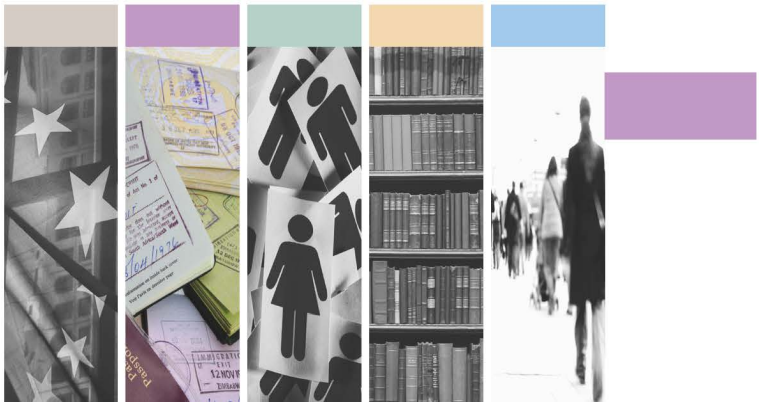
Policy Areas

- Constitutional Affairs
- Justice, Freedom and Security
- Gender Equality
- Legal and Parliamentary Affairs
- Petitions

Documents

Visit the European Parliament website:
http://www.europarl.europa.eu/supporting-analyses

PHOTO CREDIT: iStock International Inc.



ISBN 978-92-823-7998-1 (paper)
ISBN 978-92-823-7999-8 (pdf)

doi: 10.2861/1389 (paper)
doi: 10.2861/036283 (pdf)

Publications Office