The purpose and limitations of purpose limitation

PROEFSCHRIFT

ter verkrijging van de graad van doctor aan de
Radboud Universiteit Nijmegen op gezag van
de rector magnificus Prof. dr. J.H.J.M van Krieken
volgens besluit van het college van decanen,
in het openbaar te verdedigen op woensdag 23 September 2020
om 15:30 uur precies

door

Merel Elize Koning

geboren op 19 oktober 1985
te Utrecht

Promotoren:

Prof. mr. dr. M. Hildebrandt
Prof. dr. B.P.F. Jacobs

Manuscriptcommissie:

Prof. mr. dr. F.J. Zuiderveen Borgesius	
Prof. mr. dr. J.H. Gerards	Universiteit Utrecht
Prof. dr. N. Helberger	Universiteit van Amsterdam
Dr. M. Oswald	University of Northumbria, Verenigd Koninkrijk
Dr. G. Zanfir-Fortuna	Future of Privacy Forum, Detroit, Verenigde Staten

The purpose and limitations of purpose limitation

DOCTORAL THESIS

to obtain the degree of doctor
from Radboud University Nijmegen
on the authority of the Rector Magnificus prof. dr. J.H.J.M. van Krieken,
according to the decision of the Council of Deans
to be defended in public on Wednesday, September 23, 2020
at 15:30 hours

by Merel Elize Koning

born on October 19, 1985
in Utrecht (the Netherlands)

Supervisors:

Prof. mr. dr. M. Hildebrandt
Prof. dr. B.P.F. Jacobs

Doctoral Thesis Committee:

Prof. mr. dr. F.J. Zuiderveen Borgesius	
Prof. mr. dr. J.H. Gerards	Universiteit Utrecht
Prof. dr. N. Helberger	Universiteit van Amsterdam
Dr. M. Oswald	University of Northumbria, United Kingdom
Dr. G. Zanfir-Fortuna	Future of Privacy Forum, Detroit, United States

This research was conducted within the PI.Lab. https://pilab.nl/

This research was sponsored by the SIDN fonds. https://sidnfonds.nl

The author was employed at Radboud University Nijmegen. https://ru.nl

List of Abbreviations

CFREU	Charter of Fundamental Rights of the European Union
CJEU	Court of Justice of the European Union
CoE	Council of Europe
CoE R(87) 15	Recommendation (87) 15 on Regulating the Use of Personal Data in the Police Sector
dGDPR	Draft Data Protection Regulation
DPC	Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data CETS No. 108
DPD	Data Protection Directive
ECHR	European Convention on Human Rights
ECtHR	European Court of Human Rights
EDPB	European Data Protection Board
EDPS	European Data Protection Supervisor
EEA	European Economic Area
ESC	European Social Charter
EU	European Union

FIPPs	Fair Information Practice Principles
FRA	European Union Agency for Fundamental Rights
GDPR	General Data Protection Regulation
ICCPR	International Covenant on Civil and Political Rights
ISO	International Organisation for Stadardisation
LED	Data Protection Directive on Police Matters/Law enforcement Directive
ngo's	non-governmental organizations
OECD	Organisation for Economic Co-operation and Development
OECD Guidelines	OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data
PNR	Passenger name records
TEU	Treaty on the European Union
TFEU	Treaty on the Functioning of the European Union
UDHR	Universal Declaration of Human Rights
UN	United Nations
US	United States of America
WEF	World Economic Forum

Contents

Chapter 1

General introduction

1.1 Background and introduction

We live in a data-driven society. Personal data is being monetized and with the help of ubiquitous commercial surveillance infrastructures, machine learning and big data, life influenced by predictions of individual and group behavior has become normal.[1] In Europe, as elsewhere, private entities, such as big tech,[2] data brokers and online advertising companies,[3] are the engines behind the data-driven society. They collect the majority of data and make most of the computations necessary to predict and influence human behavior to benefit their commercial goals.[4] In the design decisions surrounding these new technologies and the accompanying business models, compliance with European data protection law is not always at the top of the list of design constraints.

There is an increasing interest of criminal law enforcement authorities to utilize the data and prediction models that are held by private entities for criminal law en-

[1] See [Zuboff, 2019]. Zuboff uses the term surveillance capitalism for this market development; See also https://thebaffler.com/latest/capitalisms-new-clothes-morozov for a critique by E. Morozov on the relationship that Zuboff establishes between capitalism and surveillance capitalism, as well as the way in which it prioritizes the problems of this new market form over those of capitalism itself. Lastly retrieved 22 December 2019; See also [Hildebrandt, 2008] on profiling and [Crawford, 2015] on the attention economy.

[2] Big tech is the popular name to refer to the biggest tech companies from the United States: Apple, Amazon, Google and Facebook. See for example https://www.ft.com/economics-of-big-tech. Lastly retrieved 22 December 2019; and the Surveillance Giants report of Amnesty International https://www.amnesty.org/download/Documents/POL3014042019ENGLISH.PDF Lastly retrieved 22 December 2019.

[3] See the dissertation of F.J. Borgesius Zuiderveen [Borgesius, 2014] for an analysis of the privacy protection in relation to the business models of data brokers and online advertisers.

[4] See footnote [1].

forcement purposes, specifically for the detection and prediction of crime.[5]

Private companies are offering services to criminal law enforcement authorities that include the transfer of personal data from the databases of the private entities to those of the authorities.[6] The databases of private entities are oftentimes filled with personal data that was initially collected for purposes that are incompatible with the detection, prevention or investigation of crime. Some of these commercial services are marketed directly towards criminal law enforcement agencies.[7] Other services are advertised to the general public, including criminal law enforcement agencies. Take for example the company PimEyes, that operates from Warsaw Poland and is subject to the European data protection law.[8] This company offers a search engine service that makes use of facial recognition technology. It allows its costumers, including criminal law enforcement authorities, to find pictures from all over the internet relating to an identifiable individual of interest. The costumers can buy access into the database of PimEyes to easily perform millions of searches.[9] PimEyes has been covered by the media in news articles that emphasize the dangers of facilitating online stalking via this service.[10]

Services, such as PimEyes, pose an additional societal danger: The carefully and democratically established limitations of the collection of personal data by the police under the Rule of Law can be bypassed for the amount of 0,0008 Euro per search up

[5] The detection or prediction of possible crime with the use of data is frequently referred to as *intelligence-led policing*, *data-driven policing* or *predictive policing*; In Denmark, for example, the police purchased a commercial predictive policing system that facilitates the connection of multiple databases, the collection of data from open sources and the making of predictions about criminal behavior. See https://www.information.dk/indland/2016/10/danmark-koeber-overvaagningssystem-millioner-nsa-leverandoer, and https://hoeringsportalen.dk/Hearing/Details/60330. Lastly retrieved 22 December 2019. Open source data is broadly defined by the Danish and can include bulk data that is bought from data brokers. [Jansen, 2019, p. 9]; Another example comes from the United Kingdom where police bodies also use commercial consumer behavior data in the prediction of crime. https://bigbrotherwatch.org.uk/2018/04/a-closer-look-at-experian-big-data-and -artificial-intelligence-in-durham-police/. Lastly retrieved 22 December 2019.

[6] See for example https://www.digitalmarketplace.service.gov.uk/g-cloud/services/857773661217106. Lastly retrieved 18 August 2020.

[7] See for example Clearview that markets services similar to those of PimEyes directly to law enforcement agencies. See https://clearview.ai/help/tos. Lastly retrieved 17 August 2020.

[8] See https://pimeyes.com. Lastly retrieved 17 August 2020.

[9] See https://pimeyes.com/en/privacy-policy. Lastly retrieved 17 August 2020.

[10] See for example https://www.bbc.com/news/technology-53007510 or https://netzpolitik.org/2020/pimeyes-face-search-company-is-abolishing-our-anonymity/. Lastly retrieved 17 August 2020.

to a hundred million times per month.[11] PimEyes collects the data for its database by scraping the internet. Regardless of the processing purpose at the time of uploading the picture to the internet by the original poster, PimEyes copies these pictures and analyses them by extracting the facial recognition 'fingerprint' of someone's face. The company stores these fingerprints together with a thumbnail of the original picture and metadata.[12] This personal data is stored for a period of two years in the PimEyes search engine database.[13] The costumer queries the search engine database to collect the results, and pursuits to process that data for her own purposes. These purposes will most likely be incompatible with the purposes of processing at the time when the original poster uploaded the picture to the internet, as well as incompatible with the processing purposes of PimEyes itself.[14]

Business models like these show tension with one of the core principles of data protection law: the purpose limitation principle. This principle sets forth that personal data can only be collected for specified, explicit and legitimate purposes and cannot be further processed in a manner that is incompatible with those purposes. There seems to be no general agreement about the protective value of the purpose limitation principle. Over the years the European Data Protection Boards (EDPB), the European Union (EU) body in charge of the supervision of most of the EU data protection framework,[15] emphasized the importance of the purpose limitation principle, for example, in relation to the internet of things,[16] surveillance by secret services or criminal law enforcement authorities,[17] data processing for commercial ends by

[11] Calculation retracted from https://pimeyes.com/en/api-get-started. Lastly retrieved 17 August 20.

[12] See https://pimeyes.com/en/privacy-policy. Lastly retrieved 17 August 2020.

[13] See https://pimeyes.com/en/privacy-policy. Lastly retrieved 17 August 2020.

[14] The PimEyes business operations might violate other data protection rules too, such as the processing of biometric data through the creation and storage of the fingerprint without a legitimate legal ground ex art. 9 GDPR in the PimEyes database. These aspects fall outside the scope of this study.

[15] The EDPB replaces the Article 29 Working Party. It is made up of the head of each supervisory authority and of the European Data Protection Supervisor (EDPS) or their representatives. Their opinions are non-binding but contribute to legal doctrine. See art. 68 GDPR. See also https://edpb.europa.eu/ Lastly retrieved 22 December 2019.

[16] Article 29 Working Party *Opinion 8/2014 on the Recent Developments on the Internet of Things*, 2014, WP 223, p. 7: "The user was comfortable with sharing the original information for one specific purpose, he/she may not want to share this secondary information that could be used for totally different purposes. Therefore it is important that, at each level (whether raw, extracted or displayed data), IoT stakeholders make sure that the data is used for purposes that are all compatible with the original purpose of the processing and that these purposes are known to the user".

[17] Article 29 Working Party *Working Document on surveillance of electronic communications for intelli-*

online data brokers in the behavioral advertisement industry,[18] international data exchange for taxation matters,[19] the prevention of money laundering and terrorist financing,[20] and cloud computing.[21]

Yet, the purpose limitation principle is considered controversial.[22] Some scholars see the obligation that can be derived from the principle more as a formality.[23] Other, more technology- and/or profit-oriented scholars see the limitations on data processing as a nuisance to innovation.[24] Zarsky argues, for example, that purpose limitation can be considered a disturbance of fair competition, as it "limits the abilities of start-ups to gather information on secondary markets and use it to enter new realms of business."[25] In his eyes purpose limitation "might amount to paternalism and undermines autonomy" because the European legislature is intervening in a market where the data subjects have objectively and actively surrendered much of their control over personal data to data controllers.[26] It is true that the restrictions on data processing that are posed by the purpose limitation principle interfere with the unlimited deployment of machine learning and artificial intelligence on personal data and trigger dismal reactions from people who intend to share data or do big data analysis on personal data sets.[27] In the context of big data even the United Kingdom Information

gence and national security purposes, 2014, WP 228, p. 24; Article 29 Working Party *The Future of Privacy Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data* , 2009, WP 168, p. 27.

[18] Article 29 Working Party *Opinion 2/2010 on online behavioral advertising*, 2010, WP 171, p. 20.

[19] Article 29 Working Party *Statement of the WP29 on automatic inter-state exchanges of personal data for tax purposes*, 2014, WP 230, p. 3: "any system of exchange of data, especially when it is based on automatic exchange of personal data related to a large number of individuals, should meet the data protection standard, in particular the principles of purpose limitation and necessity.".

[20] Article 29 Working Party *Opinion 14/2011 on data protection issues related to the prevention of money laundering and terrorist financing*, 2011, WP 186, p. 3: "The WP29 recommends the strict and clear application of the purpose limitation principle".

[21] Article 29 Working Party *Opinion 05/2012 on Cloud Computing*, 2012, WP 196, p. 16.

[22] Publications on the principle have titles such as: *Purpose limitation in EU-US data exchange in criminal matters: the remains of the day* [De Busser, 2009b]. or *The End of the Purpose-specification Principle in Data Protection?*.[Cannataci and Bonnici, 2010].

[23] [Nissenbaum, 2015, p. 292].

[24] See for example [Stalla-Bourdillon and Knight, 2018]; [Moerel and Prins, 2016].

[25] [Zarsky, 2016, p. 1007].

[26] [Zarsky, 2016, p. 1007] and [Zarsky, 2015].

[27] Various scholars have noted the tension between the purpose limitation principle and big data, artificial intelligence and machine learning. See for example [Hildebrandt, 2013]; [Ballaschk, 2015, p.31]; [Zarsky, 2016, p. 1005]; [Ghani et al., 2016, p. 118]. I do not want to argue in this study that these technologies only impose threats and negative effects. See [Lyon and Bauman, 2013] for a well thought-out

Commissioners Office, the supervisory authority, criticized limitations on data usage based on pre-determined terms, and instead suggested limitations on further use of personal data based on fairness and the expectations of the data subject.[28]

Frequently, the debate on the purpose limitation principle only concentrates on the non-incompatibility requirement, that obligates the data controller not to process the data for purposes that are incompatible with the ones specified at the time of the collection. However, some scholars do focus also on the purpose specification requirement, that obligates the data controller to only process personal data for legitimate, specific and explicit purposes.

This is, for example, the case in *Privacy for the homo digitalis* of Moerel and Prins.[29] Moerel and Prins rally for the discontinuation of purpose limitation as a separate criterion.[30] In their view data protection law obligates to conduct too many separate tests that have overlapping criteria at various moments of the data processing, which renders the law ineffective and unnecessarily complex.[31] On top of this, Moerel and Prins consider the purpose limitation principle failing as a data protection principle because personal data is no longer a by-product in present-day business models; it is the core commodity of many businesses in the data-driven society.[32] The authors argue that, since data collection and analysis are in itself the purpose, purpose limitation is no longer meaningful.[33] They argue that the elements of the purpose limitation

discussion on the benefits of these technologies.

[28] Report: *Big Data and data protection*, Information Commissioner's Office 2014, Available at https://rm.coe.int/big-data-and-data-protection-ico-information-commissioner-s-office/1680591220 Lastly retrieved 22 December 2019; and Report: *Big data, artificial intelligence, machine learning and data protection*, United Kingdom Information Commissioner's Office 2017, p. 37-39, Available at https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf Lastly retrieved 22 December 2019; This approach ties in with the approach of the European Court of Human Rights where the foreseeability of further data processing is assessed. Ironically the Brexit transition sparked the debate on the option of the United Kingdom leaving the European Convention of Human Rights. See [Amos, 2017] for this discussion; See also [Rodotà, 2009, p. 77].

[29] [Moerel and Prins, 2016]. The chapter was first published in Dutch in [Moerel et al., 2016] with the title *Privacy voor de homo digitalis, Proeve van een nieuw toetsingskader voor gegevensbescherming in het licht van Big Data en Internet of Things*.

[30] [Moerel and Prins, 2016, p. 42].

[31] See footnote [30].

[32] [Moerel and Prins, 2016, p. 42-43].

[33] [Moerel and Prins, 2016, p. 42-44]. The authors do not regard the purpose limitation principle to set boundaries on the data processing that uses, for example, Big Data technologies in a capitalistic society.

principle are also covered by the legitimate interest test.[34] In the authors' view the multiple tests can be abolished and the aforementioned issues will be (partly) solved when purpose limitation is replaced by the question: Is there a legitimate interest for the various data-processing activities: collection, processing, further processing and destruction?[35]

To my belief the legitimate interest test indeed partly overlaps with the compatibility test, but I also believe that the basic idea behind the interests of the data controller is fundamentally different from the idea behind purpose limitation. Moerel and Prins illustrate how the legitimate interest would function as a type of use limitation in data processing with two examples that – as it turns out – both depend on the processing purposes.[36]

In my view, such alternatives for the purpose limitation principle are unsatisfactory because the solution was not directed towards substituting the protective value of the full purpose limitation principle. Studies like the one done by Moerel and Prins appear to not take fully into account the fundamental rights framework when discussing the role of the purpose limitation principle and the values that underpin it.[37] The role of the purpose limitation principle itself as well as the role of fundamental rights when interpreting the purpose limitation principle are, in my opinion, not well understood.

An in-depth investigation into the role of fundamental rights when interpreting the purpose limitation principle is necessary, because the data protection framework does not exist in a legally secluded space. The data protection framework interacts with fundamental rights in the sense that fundamental rights norms must be translated into data protection rules, but data protection rules also influence fundamental rights law.[38] This study examines the role of the purpose limitation principle in European data protection and fundamental rights law.[39] This study has a focus on criminal

[34] [Moerel and Prins, 2016, p. 48].

[35] [Moerel and Prins, 2016, p. 46].

[36] [Moerel and Prins, 2016, p. 55-56]. In the first example the data subjects have to consent to the processing purposes and in the second example the authors state that: "A key element here is that the scan and diagnosis data would only be used to train the algorithm". This is a processing purpose and a limitation to that specific purpose and not a limitation based on the interests of the data controller.

[37] Another example is the dissertation of Maximillian von Grafenstein, who takes a risk-based approach that focusses on the role of data protection in the free and open market. [von Grafenstein, 2018].

[38] See [Fuster, 2014b] on the relationship of data protection law and the right to protection of personal data.

[39] The research questions are presented in Section 1.2.

law for two reasons: One, to anticipate on the trends of data-driven policing and private to public data transfers in the pre-crime phase of criminal law enforcement, and, two, because fundamental rights considerations come into play when data is being processed for the objectives relating to criminal law enforcement. The focus on criminal law allows us to untangle the role of the principle because, as will become clear during this study, this role is very different under the data protection framework governing private entities as it is under the framework governing the data processing by competent criminal law enforcement authorities. Also, the link between the purpose limitation principle and fundamental rights framework will become more visible when studying case law in the context of criminal law enforcement because of the distinctive character of the interferences and impact of the interferences on the rights and freedoms of individuals the context of criminal law enforcement. The study looks at how the purpose limitation principle is embedded in the regulatory framework that applies to data processing of private entities and the framework that applies to the data processing of criminal law enforcement authorities, as well as what the role of the principle is when the regulatory framework switches because data is being transferred from private entities to criminal law enforcement agencies. The purpose of this investigation is to explore the protective value of the principle so that its results can support future discussions on the purpose limitation principle in the data-driven society.

As identified on page 2, one of the challenges that the data-driven society is facing is the protection of fundamental rights and personal data in private to public data transfers in the field of criminal law enforcement. Data protection law allows derogations from the non-incompatibility requirement for the objectives of detection, prevention and investigation of crime when strict criteria are met. One criterion is that processing of personal data for incompatible purposes that pursue criminal law enforcement objectives should be based on a legislative measure. This means that the private entity must be confronted with a legal obligation to transfer the data to the criminal law enforcement authorities. But what if such an obligation is missing? What if a private entity spontaneously discloses personal data of individuals to the police because the entity suspects that the data will reveal fraudulent conspiracy?

When a private entity has discovered a signs of crime or a pattern of criminal activities in its data, the data protection framework foresees in the possibility to voluntarily transfer relevant personal data in individual cases or in several cases relating to the

same criminal act. In these cases the data controller is fulfilling its social responsibility by reporting crime to the competent authorities. But what if the private entity did not make any discovery but is confronted with a request by the police instead of a warrant, and private entity transfers bulk data to the criminal law enforcement authority? Or what if the business model of the private company includes providing criminal law enforcement authorities access to its databases, like the business model of PimEyes? In other words, what is the protective value of the purpose limitation principle in this changing data landscape of criminal law enforcement where voluntary public private partnerships are becoming more common and the focus of policing is shifting from the investigation of crime to the prediction and prevention of it?

This study is a theoretical investigation into the wider notion of the purpose limitation principle with specific emphasis on the role of the principle in private to public data transfers because as the data-driven society develops these questions will gain importance from a fundamental rights and Rule fo Law perspective. Legal scholars, practitioners and policy makers must be made aware of the purpose and limitations of the purpose limitation principle to understand its role in the upcoming area of data-driven policing in order to see where the data protection framework fails to protect the fundamental rights of the data subjects and to take appropriate action. I hope this study makes a distinct, if modest, contribution to the understanding of the foundations of European data protection law.

1.2 Central concepts and limitations

This study focusses on European data protection and fundamental rights law. The legal framework that is discussed in this study will be introduced in Chapter 2. European data protection law defines personal data as any information relating to a directly or indirectly identified or identifiable natural person.[40] Data processing means any operation that is performed on personal data.[41] For example, the questions that were identified on page 7 speak of data that is transferred by the private entity and of direct access to the databases of private entities for competent authorities. Both the transfer of personal data and the act of giving access to databases concern the pro-

[40] See article 4(1) GDPR and art. 3(1) LED.
[41] See article 4(2) GDPR and art. 3(2) LED.

cessing of personal data under European data protection law.[42] This study uses the terms *personal data* and *data* interchangeably to indicate personal data. Not all information concerns personal data. *Bulk data* can contain information that is subject to laws and regulations that fall outside the data protection domain, such as intellectual property law or export regulations. The legal ramifications of these other laws fall outside the scope of this study.

Also, sometimes the information that is processed in the data-driven society relates to personal data but is not personal data in itself. This is for example the case when a private entity shares with a competent authority a *general profile*, which is made up of descriptions of personal traits and behavior of natural persons that belong to a group of interest as well as a likelihood indication of certain other personal traits and (past, present-day and future) behavior of individuals who fit that profile.[43] Personal data is processed for the composition of general profiles, and the information from a general profile becomes personal data when it is used to single out natural persons and to add information to personal profiles. However, the general profile itself does not qualify as personal data insofar as it does not relate indirectly to one identifiable person. The purpose limitation principle is not applicable to re-use of these general profiles. Therefore, the disclosure of general profiles by commercial entities to criminal law enforcement authorities falls outside the scope of this study.[44] Nevertheless, it is important to realize that when a database with personal data is ran against a general profile, this operation does qualify as personal data processing. The purpose limitation principle only regulates situations in which personal data is processed, and, therefore, limits this study to the processing of this type of data.

The terms *competent authority* and *criminal law enforcement authority* refer to an authority competent for the prevention, detection, investigation or prosecution of criminal offenses which is established under EU Member State law.[45] The data

[42] See footnote [41].

[43] See for a good description of the commercial online profiling world the first pages of [Borgesius, 2016]; Groups of interest are, for example, zero-day exploit buyers, journalists, immigrants or Wall Street bankers. Personal traits and behavior of interest could be, for example, the likelihood to commit a cyber crime, to publish State classified information, to overstay a residence permit, or to commit a fraudulent crime. See also [Hildebrandt, 2008].

[44] Amongst other scholars F.J. Zuiderveen Borgesius identified this gap in legal protection [Borgesius, 2018]; Additional reseach into the impact on the protection of fundamental rights and freedoms is highly recommended.

[45] Study into the purpose limitation principle and data-driven crime detection by criminal law enforce-

processing by these national competent authorities falls under the scope of the Data Protection Directive on Police Matters (LED).[46] The data transfers to law enforcement authorities that lack a criminal law enforcement mandate, such as agencies charged with social security fraud detection, fall outside the scope of this study.[47]

In this study I use *the detection of crime* to refer to the *pre-crime phase of criminal law enforcement*. This phase precedes the investigation and prosecution phase of criminal law enforcement.[48] It is a phase in which uncertainty exists with regard to the existence of a crime, a suspect or a suspect population. Data of wider groups in society is processed in the pre-crime phase for the objective of detection of crime, including personal data of data subjects that have no relation to criminal activity.

In this study the term *data processing for criminal law enforcement and public security objectives* or *LED objectives* indicates that the data processing falls under the scope of the LED. The LED itself speaks of personal data processing for the *purposes* of the prevention, investigation, detection or prosecution of criminal offenses or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security ex art. 1(1) LED. I replace the word *purposes* with the word *objectives* when I refer to these "large purposes" that relate to the scope of a data protection instrument. The word *purposes* is only used in relation to the processing

ment authorities that are established under EU, such as Europol law, is recommended and could build on the conclusions of this study; See for an investigation of the implementation of the purpose limitation principle in the Europol Regulation [Coudert, 2017].

[46] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA ; For a discussion on the three traditional tasks of the police – criminal law enforcement, maintenance of public order and assistance to the general public – and the scope of the LED and the GDPR I kindly refer to Section 2.2.2.3 on page 54.

[47] It would be interesting to asses the extent to which the transfer of personal data, from private entities to these type of agencies is compatible with the legality principle in future research.

[48] The term detection of crime is sometimes used to refer to a broader concept than the pre-crime phase which includes the investigation phase.See for example *The European Convention on Human Rights and Policing, a handbook for police officers and other law enforcement officials*, Council of Europe, 2013, p. 47: "Police officers invariably enjoy certain rights incidental to their responsibilities for the detection of crime such as the power to stop and search suspects or to require a witness to remain with an officer while personal details are ascertained." Available on https://www.echr.coe.int/Documents/Handbook_European_Convention_Police_ENG.pdf. Lastly retrieved 22 December 2019; This study uses the terminology from art. 1(1) LED that distinguishes between the detection and investigation phase.

purposes that are regulated by the purpose limitation principle.

The reader should bear in mind that this study is only focussed on the purpose limitation principle, and, therefore, can only answer a small subset of questions that come to mind when considering data protection and the protection of fundamental rights in the data-driven society. This study investigates at what moment actions of a private party should be attributed to the State and when such actions interfere with the right to respect for private life. A full discussion of the horizontal effect of the rights protected in the ECHR lies beyond the scope of this study. This study also does not engage with the effect of the retrospective application of the right to a fair trial on the data collection phase when criminal charges are brought to an individual whose personal data was processed to predict crime which lead to further criminal investigation. This study will not provide a comprehensive analysis of the criminal law- and criminal law enforcement legality principle. It is also not the task of this study to include a full discussion of the data subject rights, inclusing in situations that entail automated decision making and commercial profiling. To fully understand the legality, data protection and fundamental rights implications of these issues, future research should be developed.

1.3 Research questions and terminology

The following subsections describe the vocabulary that will be used in this study, followed by the general research question and the subquestions.

1.3.1 Vocabulary to discuss the purpose limitation principle

To discuss the purpose limitation principle and its function in European data protection law a precise vocabulary is necessary, that I introduce here.

Purpose limitation principle The purpose limitation principle safeguards that personal data must be collected exclusively for specified, explicit and legitimate purposes and not processed in a manner that is incompatible with those purposes.

Purpose specification requirement The purpose specification requirement lays down that personal data must be collected only for *specified, explicit and legitimate*

purposes.

Purpose specification Purpose specification refers to the purpose statement that is given by the data controller or that is embedded in the legal measure on which the processing is based.

Processing purposes The actual purpose of a data processing operation is referred to as the processing purposes. The processing purposes can differ from the purpose specification.

Initial and new processing purposes Initial purposes are the processing purposes at the moment of data collection or re-use of personal data. New processing purposes are any secondary processing purposes that are different from the initial purposes.

Non-incompatibility requirement, compatibility assessment, compatible and incompatible purposes The non-incompatibility requirement is a type of use limitation that prohibits the processing of personal data for purposes that are incompatible with the purposes at the time of the data collection. The requirement necessitates a compatibility assessment between the initial and new processing purposes. The terms *compatible purposes* and *incompatible purposes* refer to the outcome of this compatibility assessment.

Use limitation Use limitation refers to the limitation of personal data use after the data has been collected. This study describes the various types of use limitation that are presented in European data protection law. It is important to bear in mind that in this study use limitation is an overarching concept and not a synonym for the non-incompatibility requirement.

Collection of personal data A data controller can collect personal data from the data subject or third parties, including other data controllers. The personal data can be volunteered by the data subject or observed by the data controller. The personal data can also be inferred from other data with the help of, for example, big data analysis.[49] Personal data can also be collected from other data controllers who received the

[49] [WEF, 2011, p. 18].

personal data from the data subject, or who observed the data subject, or who inferred the personal data, or who collected the data from yet another data controller.

Further processing of personal data All processing that follows the collection of personal data should be considered *further use of personal data* or *further processing*, irrespective of whether the further processing fulfills the initial purposes or new processing purposes.[50]

Processing operation A processing operation is a set of processing activities performed on personal data that starts with the lawful collection or re-use of data and continues until the purpose is exhausted.[51]

Restrictions Restrictions allow justifiable limitations on data protection principles or fundamental rights and freedoms. Restrictions should be considered an exception and can never become the general rule.

Derogations Derogations allow limitations on data protection principles. These derogations are provided in data protection law. These limitations are not considered restrictions and can therefore become the general rule.

Re-use of personal data The term re-use of personal data is used in this study to indicate a subset of further use which is based on a derogation from the non-incompatibility requirement. Re-use of personal data should be considered a new processing operation.

[50] Article 29 Working Party *Opinion on Purpose Limitation*, 2013, WP 203.

[51] This vocabulary is also used in the new regulatory framework. See for example Recital 42 GDPR; However, the CJEU has recently used processing operation in a slightly different manner. in CJEU 29 July 2019, C-40/17 (*Fashion ID GmbH & Co. KG*), par. 72 the Court explained that "processing of personal data may consist in one or a number of operations, each of which relates to one of the different stages that the processing of personal data may involve." For the sake of clarity in the text of this thesis I will refer to a *processing operation* as relating to all processing activities relating to the purpose at the start of the re-use of collection of personal data: a processing operation relates to a series of processing activities in relation to a purpose and not to one single activity.

Unlawful further processing of personal data Personal data is unlawfully further processed when it is processed for purposes that are incompatible with the initial purposes and can not be justified by a derogation from the non-incompatibility requirement. This type of data processing cannot form a new processing operation and renders the processing that is incompatible with initial purposes unlawful.

GDPR-data Personal data that has been initially collected under the scope of the GDPR.

LED-data Personal data that is processed under the scope of the LED.

Privileged purposes Purposes which are archiving purposes in the public interest, scientific and historical research purposes and statistical purposes are referred to as privileged purposes.

1.3.2 General research question

The general research question of this study is:

> What is the role of the purpose limitation principle in European data protection and fundamental rights law?

In order to formulate a precise answer to this question and to avoid overlooking functions of and limitations on aspects of the purpose limitation principle, I chose to investigate the two requirements of the purpose limitation principle, purpose specification and non-incompatibility, separately.

1.3.3 Subquestions

The study into the purpose limitation principle and its two requirements in European data protection and fundamental rights law is guided by secondary research questions. The first focus point is the notion of the purpose limitation principle when looking purely through a fundamental rights lens. It is important to understand to what extent the purpose limitation principle is connected with the material scope of the right to protection of personal data and the right to respect for private life. To

answer this question we must research if and how interferences of the purpose specification requirement, in the sense that the purposes were not regarded to be specific, explicit and legitimate, have lead to an infringement on fundamental rights. The following question will be answered:

- To what extent do limitations on the purpose specification requirement lead to infringements of fundamental rights?

Next, to understand the role of the purpose specification requirement in fundamental rights law its role in the justification of fundamental rights interferences will be studied. Special attention is given to the central role of the requirement in data protection law and how that translates to the level of fundamental rights, in particular to the concept of the essence of the right. With regard to the purpose specification requirement and its role in fundamental rights law the answers to following additional questions are investigated:

- In what way is the idea behind purpose specification connected to the justification criteria of fundamental rights infringements?
- To what extent is purpose specification connected to (the essence of) the fundamental right to respect for private life and the right to protection of personal data?

Similarly, to consider how the non-incompatibility requirement is connected to the material scope of the right to protection of personal data and the right to respect for private life, we have to investigate if an how the processing of personal data for incompatible purposes have lead to an infringement on these rights or have contributed to the justification of an infringement on these rights.

- To what extent do limitations on the non-incompatibility requirement lead to an infringement of fundamental rights?
- To what extent does further use of personal data lead to an infringement of fundamental rights?
- In what way is the non-incompatibility requirement connected to the justification criteria for fundamental rights infringements?

This study also briefly explores suggested alternatives to the purpose limitation principle and investigates what the effect of these alternatives would be on the protection of fundamental rights. During the exploration the following subquestion will be answered:

- Would the right to protection of personal data and the right to respect for private life be safeguarded if the purpose limitation principle would be replaced by other concepts to regulate the use of personal data?

The above subquestions help in providing the answer to the question what the role of the purpose limitation principle is in European fundamental rights law, but do no provide a full understanding of the role of the purpose limitation principle in European data protection law. In order understand the role of the purpose limitation principle in European data protection law other subquestions lead the research. The subquestions that will be addressed in this study are:

- What is the role of the purpose specification requirement in data protection law?
- What is the role of the non-incompatibility requirement in data protection law?

To answer these questions the perceived notions of the purpose specification requirement and the non-incompatibility requirement in data protection doctrine are studied, as well as the position of the two requirements in data protection law, their relationships with other data protection principles and rules, and the direct and indirect discussion of the purpose limitation principle in relevant case law.

To form a deeper understanding of role of the principle in data protection law it is also important to understand the conceptual relationship between its two requirements and its position compared to other data protection principles within data protection law. Therefore, this study also seeks the answers to the following questions:

- What is the relationship between the purpose specification requirement and the non-incompatibility requirement?
- What is the position of the purpose limitation principle as a data protection principle compared to the position of the other data protection principles?

The non-incompatibility requirement limits the use of personal data based on the compatibility of purposes. We want to know if there are other lawful types of use limitation in data protection law and what the position of the non-incompatibility requirement is in relation to these other types of use limitation. The following questions are included in this study:

- What other types of limitations on data processing are implemented in European data protection law?
- How does the non-incompatibility requirement relates to these other types of use limitation?

To fully understand the role of the purpose specification requirement its relationship with these other types of use limitation is studied too. Therefore, the additional subquestion that must be answered in order to understand the role of the purpose limitation principle in data protection law is:

- What is the relationship between the purpose specification requirement and these other types of use limitation?

Answering the above subquestions will provide the answer to the general research question: What is the role of the purpose limitation principle in European data protection and fundamental rights law? This general research question is theoretical and needed to be answered to investigate to what extent the re-use of commercially collected GDPR-data for purposes that pursue criminal law enforcement objectives in the pre-crime phase of law enforcement by competent authorities is legitimate under European dat protection and fundamental rights law. First we have to understand if there are specific arrangements in the European data protection framework that oversee voluntary data transfers from private entities to criminal law enforcement authorities. This research will be lead by the following subquestion:

- How are voluntary data transfers of GDPR-data for LED objectives regulated in the European data protection framework?

To know what the role of the purpose limitation principle is in private to public data transfers in the pre-crime phase of criminal law enforcement, we have to investigate to what extent private entities have the power to influence the further processing

of personal data that have been voluntarily transferred. The following questions will be answered:

- To what extent can private entities determine the processing purposes and restrict the processing by the criminal law enforcement authority after data is voluntarily transferred?
- Do the purposes of processing of the private entity affect the lawfulness of the data collection by the criminal law enforcement authority when this data is voluntarily transferred by the private entity?

Lastly, from a fundamental rights perspective, the voluntary data transfers beg the question at what time the data processing of a private entity falls under the accountability of the government and what criteria does the ECtHR deploy to make this assessment.

- Under which conditions stemming from fundamental rights law does processing by a private entity of data that is intended for transfer to a competent authority fall under the accountability of the government?

1.4 Method and structure

This research is based on desk research, drawing on the relevant sources of law: legislation, case law, opinions and guidelines of the EDPB and other advisory bodies, and doctrine. The research heavily relies on case law analysis and legislative documents for the simple fact that limited literature on the purpose limitation principle has been published. This study focusses on European law at the level of the Council of Europe (CoE) and the EU. Answers to the research questions at this level will benefit legal scholars, practitioners and policy makers throughout Europe and enable scholars to use the results of this study as input for legal comparative studies with other data protection frameworks elsewhere in the world.

The focus on the EU and CoE has been chosen because of the interesting interactions between EU secondary data protection law and European fundamental rights law in the past decades. The author systematically researched the case law on data protection, public private partnerships and data processing in the context of criminal

law enforcement with the CJEU and the ECtHR. The study relies primarily on primary sources because it analyses case law through the lens of the purpose limitation principle. Some of the analyzed case law has been extensively discussed in secondary literature before. These previous discussions, however, did not focus on the relationship between the purpose limitation principle and fundamental rights law. For this reason, references to these discussions are limited in this study.

Traditionally, the purpose limitation principle is investigated as one principle. I copied this method for the literature study, which forms the base of Chapter 3 on the general notion of the purpose limitation principle. For the law and case law study the two requirements of the principle, purpose specification and non-incompatibility, are investigated separately. The benefit of this approach is that this allows me to untangle the distribution of the protective value of the principle between the requirements, which will be necessary to describe the function of the principle as a whole. The thesis takes a descriptive approach.

The study is organized like this:

Chapter 1 introduces the background to the discussion on the value of purpose limitation, the central concepts in this study, and the research question and terminology.

The next four chapters concern the theoretical framework. Chapter 2 describes the relevant legal framework, starting with the fundamental rights framework and ending with the data protection framework.

Chapter 3 is concerned with the general notion of the purpose limitation principle. It starts with a description of the function of purpose limitation and different terminology and definitions that are used to describe the principle in the literature on data protection. This chapter continues by laying out the different elements of the purpose limitation principle, the higher goal of purpose limitation, the position of the principle in data protection law and its interaction with other data protection touchstones.

Chapter 4 focusses on the purpose specification requirement. It traces down the interrelationship with other concepts, rules and principles in data protection with the purpose specification requirement, the purpose specification and the processing purposes. Next, the chapter looks at how purpose specification is connected to the jus-

tification criteria for fundamental rights violations: legitimate aim, legality, necessity and proportionality and respect for the essence of the right.

Chapter 5 is the last chapter of the theoretical framework. This chapter investigates how the further use of personal data is regulated in data protection and fundamental rights law. It begins with an in-depth analysis of the non-incompatibility requirement in data protection law and the case law. Section two concerns the first lawful derogation from the non-incompatibility requirement: re-use based on a *lex specialis* as required in art. 6(4) GDPR. The third section investigates the second lawful derogation from the non-incompatibility requirement: re-use based on renewed consent. Section four presents (the lack of) European data protection law that regulates the re-use of commercial GDPR-data for LED objectives like the detection of crime. Section five is concerned with the investigation of the lawful derogation from the non-incompatibility requirement under the LED and looks at the effects of this derogation on the default use limitation in the field of criminal law enforcement and public security. Next, the lawful re-use of personal data for a selected group of privileged purposes is discussed. The final section of this chapter unravels the type of use limitation that is based on stringent interpretations of the purpose specification that is either stipulated by the legislature or the data controller.

Chapter 6 ties the results from the previous four chapters together and formulates the answers to subquestions and the general research question of this study. Chapter 7 suggests two recommendations that are addressed to civil society and the European legislature. Based on the conclusions and recommendations the future research areas are identified in Chapter 8.

This study closes with the bibliography, list of case law, list of consulted opinions and recommendation from the European Data Protection Board, and my résumé.

Chapter 2

Relevant legal framework

This chapter discusses the relevant data protection and fundamental rights framework that applies to private-to-public data transfers for the detection of crime. The first sections consider the fundamental rights framework, most notably art. 8 European Convention of Human Rights and art. 7 and 8 Charter of Fundamental Rights of the European Union. These sections of this chapter discuss the protection that is offered by these provisions in light of data processing and public-private partnerships. The later sections discuss specific data protection law, including the Data Protection Convention of the Council of Europe and the EU data protection rules that are applicable to competent authorities of EU member States and private entities in public-private partnerships. This chapter also references some relevant non-binding data protection law.

2.1 Fundamental rights framework

The European legal order is pluralistic. It constitutes of a supranational-, international- and national dimension. European fundamental rights law is far from a neatly organized whole or comprehensive analytical system.[52] Yet, it functions and gains constitutional importance through the shared fundamental rights aspirations of the European Union, the Council of Europe, the EU Member States and the courts of law, including the European Court of Human Rights, the Court of Justice of the European Union and national courts. These aspirations have led to the establishment of the Rule of Law in Europe: a common set of norms is determined and the interpretation of these norms is now subject to political debates.[53] In the fundamental rights dimen-

[52] [Krisch, 2008, p. 184]; [Douglas-Scott, 2014, p. 629].

[53] Various scholars have argued that the supremacy of the interpretation of norms in a streamlined constitutional hierarchy is the final step in establishing the Rule of Law. [Krisch, 2008, p. 185]; See also

sion, the European Convention on Human Rights and the Charter of Fundamental Rights of the EU are the most important legal instruments. The next subsections describe these.

2.1.1 European Convention on Human Rights

The European Convention on Human Rights (ECHR) was drafted in reaction to the human right violations of the second world war and entered into force in 1953. It is an international treaty under the wings of the Council of Europe in which the Signatory States commit to secure fundamental civil and political rights to everyone within their jurisdiction.[54] The European Court of Human Rights (ECtHR) is attached to the Convention as an international court to rule on alleging violations of the fundamental rights set out in the ECHR.[55] The following subsection gives an introduction on the notion of private life and data protection in the ECtHR's case law.

2.1.1.1 The right to respect for private life

Article 8 of the ECHR protects the right to respect for private and family life, home and correspondence.[56] The ECtHR approaches the Convention as *a living instrument*, and has built a substantive doctrine based on *the right to respect for private life* in data processing matters.[57] In fleshing out the guaranteed rights under the Convention, present-day conditions play an important role.[58] The Court consistently considers the rapid technological development of modern society.[59] In the *Szabó and Vissy*-case, for example, the ECtHR acknowledged that it is a logical consequence of technological development that governments resort to cutting-edge technologies in pre-empting emerging threats, including the massive monitoring of communications susceptible to containing indications of impending incidents, such as terrorist attacks.[60] The Court

[Licht et al., 2007] and [Risse and Ropp, 1999].

[54] [Moravcsik, 2000].

[55] The Court was established in 1959 on the basis of art. 19 ECHR.

[56] See for a study into the structure of the fundamental rights [Gerards and Senden, 2009].

[57] ECtHR 6 September 1978, no. 5029/71 (*Klass and others/Federal Republic of Germany*); and ECtHR 16 December 1992, no. 13710/88 (*Niemietz/Federal Republic of Germany*).

[58] ECtHR 25 April 1978, no. 5856/72, (*Tyrer/the United Kingdom*) par. 31.

[59] ECtHR 11 July 2002, no. 28957/95, (*Christine Goodwin/the United Kingdom*), par. 75; See for example ECtHR 4 December 2008, no.130562/04 and 30566/04 (*S. and Marper/the United Kingdom*), par. 70-71.

[60] ECtHR 6 June 2016, no.37138/14 (*Szabó and Vissy/Hungary*), par. 68.

explained that in the face of the progress of widespread automated and systemic data collection, it will scrutinize the question whether the development of surveillance methods has been accompanied by a simultaneous development of legal safeguards securing respect for citizens' Convention rights.[61] The ECtHR stressed that, overall, present-day conditions call for different and new approaches to the risk of harm posed by technology.[62] These conditions have occasionally led to positive obligations[63] on the contracting parties to prevent infringements by government bodies or private entities, or obligations to ensure that contracting parties are equipped with powers to control, prevent and investigate these infringements.[64]

[61] ECtHR 6 June 2016, no.37138/14 (*Szabó and Vissy/Hungary*), par. 68.

[62] The 2013 *Węgrzynowski and Smolczewski*-case is an example of this. That case dealt with the right to be forgotten and internet archives. Court underlined that 'the Internet is an information and communication tool particularly distinct from the printed media, especially as regards the capacity to store and transmit information. [...] The risk of harm posed by content and communications on the Internet to the exercise and enjoyment of human rights and freedoms, particularly the right to respect for private life, is certainly higher than that posed by the press'. ECtHR 16 July 2013, no. 33846/07 (*Węgrzynowski and Smolczewski/Poland*) par. 58; At the moment of finishing this study the *Big Brother Watch*-case is referred to the grand chamber of the ECtHR. The First Section of the ECtHR explained that when it comes to present-day conditions: "[...] the Court does not doubt the impact of modern technology on the intrusiveness of interception, and has indeed emphasized this point in its case-law, it would be wrong automatically to assume that bulk interception constitutes a greater intrusion into the private life of an individual than targeted interception, which by its very nature is more likely to result in the acquisition and examination of a large volume of his or her communications. ECtHR 13 September 2018, nos. 58170/13, 62322/14 and 24960/15 (*Big Brother Watch and others/the United Kingdom*), par. 316; See also P. Korenhof's forthcoming dissertation on an elaborate study of the problems underlying the demand for such a right, with the working title *Let's forget about it: the web of problems for the right to be forgotten*, as will be available on https://www.korenhof.eu/.

[63] See for a study into the development of positive rights under the ECHR by the ECtHR [Mowbray, 2004].

[64] In the *K.U./Finland*-case, for example, an unidentified person placed an sex advertisement, that included personal data, on an Internet dating site in name of a 12 year old boy, without his knowledge. The advertisement exposed the boy to sexual predators on online fora. This happened in the year 1999: the midst of the dot-com bubble, yet a moment when Internet regulation was far from comprehensive. The Finnish law enforcement authorities and investigative judges lacked the power to obtain information from the ISP that could lead to the identity of the third person who posted the advertisement. Taking into account these present-day conditions the court explained that 'the State's positive obligations under Article 8 to safeguard the individual's physical or moral integrity may extend to questions relating to the effectiveness of a criminal investigation'. The court noted, however, that in view of the difficulties involved in policing modern societies, the obligations under Article 8 to safeguard an individual's physical or moral integrity must be interpreted in a way that does not impose an impossible or disproportionate burden on the authorities. ECtHR 2 December 2008, no. 2872/02 (*K.U./Finland*), par. 46. In their turn, positive

The ECtHR's case law shows that *private life* is a broad term that is not susceptible to exhaustive definition.[65] This broad scope includes the right to identity and personal development, as well as the right to establish and develop relationships with other human beings and the outside world.[66] Private life may even include activities of a professional or business nature.[67] There is, therefore, a zone of interaction of a person with others, even in a public context, which may fall within the scope of *private life*.'[68] This zone is larger when the applicant holds the status of an ordinary individual, a john in the street,[69] and the fact that someone is the subject of criminal proceedings does not strip her from the rights as laid down in art. 8(1) ECHR.[70] Any interference under the first paragraph of art. 8 ECHR must be justified in terms of the criteria that are laid down in the second paragraph. Interferences must be in accordance with the law, necessary in a democratic society, and pursue a legitimate aim.[71] These criteria are discussed in light of the purpose limitation principle in Section 4.2, and 5.2.2.3.

---

policies have to respect the guarantees of the Convention too, specifically when it comes to powers to control, prevent and investigate crime. Such powers have to be exercised in a manner which fully respects the due process and other guarantees which legitimately place restraints on criminal investigations and bringing offenders to justice, including the guarantees of the Convention on which offenders themselves can rely on.ECtHR 2 December 2008, no. 2872/02 (*K.U./Finland*), par. 48.

[65] See for example ECtHR 7 July 2003, no. 63737/00 (*Perry/the United Kingdom*), par. 36; and ECtHR 4 May 2000, no. 30194/09 (*Shimovolos/Russia*) par. 64. Private life is not limited to the protection of an *inner circle* in which the individual may live his own personal life as he chooses and to exclude therefrom entirely the outside world not encompassed within that circle. ECtHR 16 December 1992, no. 13710/88 (*Niemietz/Federal Republic of Germany*), par. 29.

[66] See for example: ECtHR 25 September 2001, no.44787/98 (*P.G. and J.H./the United Kingdom*), par. 56; and EComHR 31 January 1995, no. 18395/91 (*Friedl/Austria*), par. 45.

[67] ECtHR 16 December 1992, no. 13710/88 (*Niemietz/Federal Republic of Germany*), par. 29; and ECtHR 25 June 1997, no. 20605/92 (*Halford/the United Kingdom*) par. 44.

[68] ECtHR 24 June 2004, no.59320/00 (*Von Hannover/Germany*), par. 50-53; See for example ECtHR 7 July 2003, no. 63737/00 (*Perry/the United Kingdom*), par. 36; and ECtHR 4 May 2000, no. 30194/09 (*Shimovolos/Russia*) par. 64; ECtHR 28 January 2003, no. 44647/98 (*Peck/the United Kingdom*), par. 57; and ECtHR 25 September 2001, no.44787/98 (*P.G. and J.H./the United Kingdom*), par. 56.

[69] ECtHR 17 May 2016, nos. 33677/10 and 52340/10 (*Fürst-Pfeifer/Austria*), par. 46; ECtHR 20 September 2018, no. 18925/09 (*Jishkariani/Georgia*), par. 51.

[70] The rights are not stripped away but the aspect of criminal proceedings can justify interferences. ECtHR 11 January 2005, no. 50774/99 (*Sciacca/Italy*), par. 29.

[71] See for example ECtHR 7 July 2015, no. 28005/12 (*M.N. and others/San Marino*), par. 71; or ECtHR 18 May 2010, no. 26839/05 (*Kennedy/the United Kingdom*), par. 130.

2.1.1.2 Data relating to private life

The next sections contribute to the answer to the questions: "To what extent do limitations on the purpose specification requirement lead to infringements of fundamental rights?" and "To what extent does further use of personal data lead to an infringement of fundamental rights?". The ECtHR never derived from any of the Convention rights an independent fundamental right to protection of personal data.[72] It did, however, acknowledge the fundamental importance of data protection for effective exercise of one's right to respect for private life and pointed to various stages at which data protection issues may arise under the scope of art. 8 ECHR.[73] In the late 1980s the ECtHR began ruling on such cases.[74] The 1987 *Leander*-case, for example, dealt with a secret police register that contained information relating to the applicant's private life. The court explained that "both the storing and the release of such information, which were coupled with a refusal to allow the applicant an opportunity to refute it, amounted to an interference with his right to respect for private life" as guaranteed by art. 8(1) ECHR.[75]

From the *Leander*-case onwards the ECtHR deploys the category of *data relating to the private life* in order to determine if data processing falls under the protective scope of art. 8(1) ECHR.[76] The scope of *data relating to the private life* is determined by a plethora of criteria that are applied by the ECtHR in a dynamic and progressive manner. These criteria can be treated under three headings: the legal qualification of the data, the type of data and the type of data processing. The following paragraphs discuss these three groups.

[72] [Fuster, 2014b, p. 99]; [Gutwirth and de Hert, 2009, p. 24-26].

[73] ECtHR 13 November 2012, no. 24029/07 (*M.M./the United Kingdom*), par. 195; ECtHR 26 January 2017, no. 42788/06 (*Surikov/Ukrain*), par. 74; In the *Peck*-case the ECtHR also noted that the protection of personal data is of fundamental importance to a person's enjoyment of her right to respect for private life and that the domestic law must therefore afford appropriate safeguards.ECtHR 28 January 2003, no. 44647/98 (*Peck/the United Kingdom*), par. 78. This is oftentimes repeated by the Court. See for example ECtHR 6 June 2016, no.37138/14 (*Szabó and Vissy/Hungary*), par. 73.

[74] In present privacy doctrine, the *Malone*-case would mark the first one. However, the ECtHR did not, at that time, recognize the data protection issues and ruled the case on issues concerning interception of mail and telephone conversations. The concurring opinion of Judge Pettiti underlines the data protection aspects. ECtHR 2 Augustus 1984, no. 8691/79 (*Malone/the United Kingdom*).

[75] ECtHR 26 March 1987, no. 9248/81, (*Leander/Sweden*) par. 48.

[76] See for example: ECtHR 16 February 2000, no. 27798/95 (*Amann/Switzerland*) par. 65; ECtHR 13 November 2012, no. 24029/07 (*M.M./the United Kingdom*) par. 187.

2.1.1.2.1 Legal qualification of the data The ECtHR distinguishes between three special legal regimes for data relating to private life: a regime for *personal data*, one for special categories of data, also known as sensitive data,[77] and one for data relating to a criminal record. Where data qualifies as personal data the ECtHR takes into consideration whether the impugned measure amounts to processing of a nature to constitute an interference with respect for private life.[78] The qualification *personal data* is, therefore, important, but not decisive in this phase of the ECtHR's assessment.[79] Medical data, in particular mental health data, is underlined by the ECtHR as highly sensitive personal data, regardless of whether it is indicative of a particular medical diagnosis.[80] Collection, storage, disclosure and other types of processing of this type of sensitive data falls, therefore, automatically within the ambit of art. 8(1) ECHR.[81] Similar weight is given to other special categories of data, such as data revealing racial origin, political opinions or religious or other beliefs, as well as personal data concerning sexual life.[82] Data relating to criminal records also directly qualifies as data that falls under the scope of art. 8(1) ECHR.[83]

[77] See Section 4.1.2.4 on page 99 for a discussion of the lawfulness of the processing of sensitive data and its connection with the purpose specification requirement.

[78] ECtHR 2 September 2010, no. 35623/05 (*Uzun/Turkey*) par. 47; and ECtHR 7 July 2003, no. 63737/00 (*Perry/the United Kingdom*), par. 40-41.

[79] The *Gaskin*-case, for example, concerned data relating to private life that did not necessarily qualified as personal data. The central question in that case was not whether or not the data related to the applicant but rather to what extent the refusal of access to the data had impact on the private life of the applicant. ECtHR 7 July 1989, no. 10454/83 (*Gaskin/the United Kingdom*); See also the *S. and Marper*-case, in which the ECtHR briefly mentions that the contested data constitutes personal data within the meaning of the Data Protection Convention as it relates to identified or identifiable individuals. The ECtHR then uses different criteria in a more in depth examination of whether the retention of the data interfered with the applicants' right to respect for their private lives. ECtHR 4 December 2008, no.130562/04 and 30566/04 (*S. and Marper/the United Kingdom*) par. 68-69; See also ECtHR 13 November 2012, no. 24029/07 (*M.M./the United Kingdom*) par. 188; ECtHR 18 November 2008, no. 22427/04 (*Cemalettin Canli/Turkey*) par. 34.

[80] ECtHR 25 February 1997, no. 22009/93 (*Z/Finland*), par. 95; ECtHR 23 February 2016, no. 40378/06 (*Y.Y./Russia*), par. 38; ECtHR 29 April 2014, no. 52019/07 (*L.H./Latvia*), par. 56; ECtHR 30 October 2012, no. 57375/08 (*P. and S./Poland*), par. 128.

[81] ECtHR 26 January 2017, no. 42788/06 (*Surikov/Ukrain*), par. 75; ECtHR 23 February 2016, no. 40378/06 (*Y.Y./Russia*), par. 57.

[82] See for example ECtHR 6 June 2013, no. 1585/09 (*Avilkina/Russia*); ECtHR 15 April 2014, no. 50073/07 (*Radu v. the Republic of Moldova*); ECtHR 29 April 2014, no. 52019/07 (*L.H./Latvia*).

[83] See for example: ECtHR 4 May 2000, no. 28341/95 (*Rotaru/Romania*), par. 43-46; ECtHR 13 November 2012, no. 24029/07 (*M.M./the United Kingdom*) par. 188; and ECtHR 17 December 2009, no. 5335/06 (*B.B./France*), par. 56.

2.1.1.2.2 Type of data The rulings of the ECtHR show that different types of data can be qualified as data relating to private life, for example, communication data,[84] financial data,[85] information that leads to personal identification and linking to a family,[86] DNA profiles,[87] fingerprints,[88] photographs,[89] CCTV footage,[90] a collection of various pieces of information that are gathered over a long period for time,[91] information derived from the monitoring of personal internet usage,[92] and data about movement in public spaces.[93]

2.1.1.2.3 Type of data processing Various types of data processing can give rise to private life considerations too, such as storage and release of data relating to private life, and systematic collection, including data collection of voluntarily provided data, publicly available data and other forms of collection without the use of covert surveillance methods.[94] The tension between *public* and *private* has repeatedly been

[84] ECtHR 1 July 2008 , no.58243/00 (*Liberty and others/the United Kingdom*) and ECtHR 6 June 2016, no.37138/14 (*Szabó and Vissy/Hungary*).

[85] ECtHR 27 April 2017, no. 73607/13 (*Sommer/Germany*), par. 47; ECtHR 7 July 2015, no. 28005/12 (*M.N. and others/San Marino*), par. 51-55; ECtHR 6 December 2012, no. 12323/11 (*Michaud/France*), par. 90-92; ECtHR 7 July 2015, no. 28005/12 (*M.N. and others/San Marino*), par. 51; See also ECtHR 16 February 2000, no. 27798/95 (*Amann/Switzerland*), par. 65.

[86] ECtHR 16 November 2004, no. 29865/96(*Ünal Tekeli/Turkey*), par. 42.

[87] ECtHR 4 December 2008, no.130562/04 and 30566/04 (*S. and Marper/the United Kingdom*); ECtHR 4 June 2013, no. 7841/08 (*Peruzzo en Martens/Germany*).

[88] EComHR 7 December 2006, no. 29514/05, (*van der Velden/the Netherlands*).

[89] ECtHR 11 January 2005, no. 50774/99 (*Sciacca/Italy*).

[90] ECtHR 28 January 2003, no. 44647/98 (*Peck/the United Kingdom*).

[91] For example in the *Roratru*-case the ECtHR notes that the a letter contained various pieces of information about the applicant's life, in particular his studies, his political activities and his criminal record, some of which had been gathered more than fifty years earlier. In the ECtHR's opinion, such information, when systematically collected and stored in a file held by agents of the State, falls within the scope of *private life* for the purposes of Article 8(1) of the Convention. ECtHR 4 May 2000, no. 28341/95 (*Rotaru/Romania*), par. 44.

[92] ECtHR 3 April 2007, no. 62617/00 (*Copland/the United Kingdom*), par. 41.

[93] For example location data from GPS trackers ECtHR 2 September 2010, no. 35623/05 (*Uzun/Turkey*), par. 52; and database surveillance of public transport ECtHR 4 May 2000, no. 30194/09 (*Shimovolos/Russia*), par. 66.

[94] ECtHR 13 November 2012, no. 24029/07 (*M.M./the United Kingdom*), par. 187; ECtHR 25 September 2001, no.44787/98 (*P.G. and J.H./the United Kingdom*), par. 57; ECtHR 18 November 2008, no. 22427/04 (*Cemalettin Canli/Turkey*), par. 33; ECtHR 16 February 2000, no. 27798/95 (*Amann/Switzerland*), par. 65-67, 69; ECtHR 6 June 2006, no. 62332/00 (*Segerstedt-Wiberg and others/Sweden*), par. 72; ECtHR 4 May 2000, no. 28341/95 (*Rotaru/Romania*), par. 43; ECtHR 26 March 1987, no. 9248/81, (*Leander/Sweden*), par. 48; ECtHR 4 December 2008, no.130562/04 and 30566/04 (*S. and Marper/the United Kingdom*),

under the scrutiny of the ECtHR because there are many occasions in which people knowingly or intentionally involve themselves in activities which are or may be recorded or reported in a public manner. In those instances a person's reasonable expectations as to privacy may be a significant – although not necessarily conclusive – factor.[95] For example, any person walking along the street will inevitably be visible to any member of the public who is also present. Monitoring by technological means of the same public scene is considered of a similar character by the ECtHR.[96] For this reason the ECtHR has held that the normal use of security cameras as such, whether in the street or on public premisses, do not raise an issue under art. 8(1) ECHR when the monitoring serves a legitimate and foreseeable purpose.[97] Private-life considerations do arise once any systematic or permanent record comes into existence of monitoring public premisses or when the recording is processed in a manner or degree beyond that normally foreseeable.[98] The fact that data is initially collected by private entities and only later used by public authorities is of little influence in this phase of the assessment.[99] The compilation of personal data profiles also falls under the scope of art. 8(1) ECHR, and the ECtHR has previously regarded the interference more severe

par. 67; ECtHR 18 October 2011, no.16188/07 (*Khelili/Switzerland*), par. 55.

[95] ECtHR 7 July 2003, no. 63737/00 (*Perry/the United Kingdom*) par. 37-38; ECtHR 25 September 2001, no. 44787/98 (*P.G. and J.H./the United Kingdom*) par. 57; ECtHR 18 October 2016, no. 61838/10 (*Vukota-Bojić v. Switzerland*), par. 54.

[96] EComHR 14 January 1998, no. 32200/96 (*Herbecq and the Association 'Ligue des Droits de l'homme'/Belgium*).

[97] ECtHR 7 July 2003, no. 63737/00 (*Perry/the United Kingdom*), par. 38; ECtHR 18 October 2016, no. 61838/10 (*Vukota-Bojić v. Switzerland*), par. 55.

[98] ECtHR 25 September 2001, no.44787/98 (*P.G. and J.H./the United Kingdom*), par. 57; ECtHR 28 January 2003, no. 44647/98 (*Peck/the United Kingdom*), par. 58-59; ECtHR 7 July 2003, no. 63737/00 (*Perry/the United Kingdom*), par. 38; ECtHR 2 September 2010, no. 35623/05 (*Uzun/Turkey*), par. 44; ECtHR 18 October 2016, no. 61838/10 (*Vukota-Bojić v. Switzerland*), par. 55.

[99] See for example ECtHR 8 April 2003, no. 39339/98 (*M.M./the Netherlands*); or ECtHR 18 October 2016, no. 61838/10 (*Vukota-Bojić v. Switzerland*). In the *Vukota-Bojić*-case the ECtHR observed that the applicant was systematically and intentionally watched and filmed by professionals acting on the instructions of a government owned insurance company on four different dates over a period of twenty-three days. The material obtained was stored and selected and the captured images were used as a basis for an expert opinion and, ultimately, for a reassessment of insurance benefits. The permanent nature of the footage and its further use in an insurance dispute was regarded as processing or collecting of personal data disclosing an interference with 'private life' within the meaning of Article 8(1) ECHR. ECtHR 18 October 2016, no. 61838/10 (*Vukota-Bojić v. Switzerland*), par. 58-59; See on covert surveillance by a private employer of employees ECtHR 5 October 2010, no. 420/07 (*Köpke/Germany*), and ECtHR 8 April 2003, no. 39339/98 (*M.M./the Netherlands*), pa. 36-43.

when such profiles include information of a person's distant past.[100] Data processing is considered particularly invasive where technology assists in acquiring detailed profiles of intimate aspects of an individual's live.[101]

To conclude, the ECtHR takes into account present-day conditions when assessing the scope of art. 8(1) ECHR. The right to respect for private life is a dynamic right and is not susceptible to a narrow definition. In assessing cases that hold data protection aspects under the right to respect for private life, the ECtHR developed a concept of *data relating to the private life of individual*. Whether or not data processing falls within the scope of this concept, and therefore within the ambit of art. 8 ECHR is determined by the legal qualification of the data, the type of data and the type of data processing.

2.1.1.3 Data protection principles and the right to respect for private life

The existence of data protection safeguards do not annul the claim to the right for respect for private life. Consent, for example, cannot deprive an individual of the protection afforded by the Convention. When an individual agreed to collection, further processing or disclosure of information, her rights under the Convention are not waived.[102]

So far, the ECtHR has only made an explicit reference to the purpose limitation principle once.[103] In that case the court noted that the domestic courts correctly iden-

[100] ECtHR 4 May 2000, no. 28341/95 (*Rotaru/Romania*), par. 43; ECtHR 2 September 2010, no. 35623/05 (*Uzun/Turkey*), par. 45; ECtHR 18 October 2016, no. 61838/10 (*Vukota-Bojić v. Switzerland*), par. 56.

[101] ECtHR 6 June 2016, no.37138/14 (*Szabó and Vissy/Hungary*), par. 70.

[102] See for example: ECtHR 13 November 2012, no. 24029/07 (*M.M./the United Kingdom*) par. 189. About free will and consent the ECtHR: 'The Government referred several times in their written submissions to the fact that the applicant herself disclosed details of the caution to her prospective employer, and that the details she disclosed were merely confirmed by the Criminal Records Office. The ECtHR observes that the posts for which the applicant applied were subject to vetting. In this context she was asked for details of her conviction and caution history and provided them as requested. The ECtHR notes and agrees with the comments of Lords Hope and Neuberger, to the effect that the fact that disclosure follows upon a request by the data subject or with her consent is no answer to concerns regarding the compatibility of disclosure with Article 8 of the Convention. Individuals have no real choice if an employer in their chosen profession insists, and is entitled to do so, on disclosure: as Lord Hope noted, consent to a request for criminal record data is conditional on the right to respect for private life being respected [...]. The applicant's agreement to disclosure does not deprive her of the protection afforded by the Convention.

[103] This case concerned the monitoring of internet use and of electronic communications in the work-

tified the interests at stake and the applicable data protection principles, including the principles of necessity, purpose specification, transparency, legitimacy, proportionality and security, as set forth in the Data Protection Directive.[104] This odd one set aside, the ECtHR usually methodically omits the words *purpose limitation*, *use limitation*, *non-incompatibility*, *purpose specification* in the sections *as to the law* and *the law*, that deliver the ECtHR's reasoning.[105] Nevertheless, in the appraisal of the scope of art. 8(1) ECHR the ECtHR does take into consideration aspects that are regulated by the purpose limitation principle in data protection law. This is specifically the case for aspects that relate to the non-incompatibility requirement in cases where private-life considerations are identified by the ECtHR for cases that would nowadays fall under the scope of the GDPR. The connection between the purpose specification requirement and the restriction clause of art. 8(2) ECHR is discussed in Section 4.2 of this study. In Section 5.1.3 the fundamental rights framework surrounding factors of the compatibility assessment are investigated. The fundamental rights safeguards in data protection rules on re-use of personal data are discussed in Section 5.2.2.3.

2.1.1.4 The application of the ECHR to data processing of private entities

The questions that were posed on page 7 discussed different levels of engagement of the competent authority in the data processing of the private entity for the detection of crime. In voluntary data transfers from private entities to competent authorities different factors can describe the engagement of the private entity in the data processing of the competent authority and *vice versa*. Data can be transferred on a structural or *ad hoc* base, the private entity can spontaneously disclose the data, the competent authority can request voluntary disclosure or the parties can enter into a commercial agreement where the data is disclosed as a paid service by the private entity.

Specifically, in the detection of complex forms of crime, such as international organized crime and cybercrime, public-private partnerships have become common. In these public-private partnerships the lines between data controller or data processor can become blurred when data is simultaneously being processed to detect crime and the competent authorities have influence on this process. The following subsections

place. ECtHR 5 September 2017, no. 61496/08 (*Bărbulescu/Romania*).

[104] ECtHR 5 September 2017, no. 61496/08 (*Bărbulescu/Romania*), par. 131. See Section 2.2.2.1 on page 49 on the GDPR that replaced the Data Protection Directive.

[105] As well as other other related terminology that was discussed in Section 3.2 on page 59.

will contribute in finding an answer to the questions: " Do the purposes of processing of the private entity affect the lawfulness of the data collection by the criminal law enforcement authority?", and "Under which conditions stemming from fundamental rights law does processing by a private entity of data that is intended for transfer to a competent authority fall under the accountability of the government?".

The following subsections describe the effects of private entity involvement to the application of the ECHR and the accountability of Signatory States.

2.1.1.4.1 Private law claims and the applicability of fundamental rights When criminal law enforcement authorities team up with private entities to combat crime the infrastructure that is used for the detection and investigation of criminal offenses frequently belongs to the private entities. The ECtHR is regularly confronted with arguments for limited applicability of the Convention rights that are based on private law, such as the law of contract. These arguments usually do not find a sympathetic response in Strasbourg. The ECtHR explained on multiple occasions that the scope of the right to respect for private life is not connected to ownership of the infrastructure or the medium on which information is processed.[106] Article 8 ECHR applies regardless of whether surveillance is carried out on a device belonging to the applicant or to a third party.[107] This ties in with the tradition of the ECtHR to assess infringements on the basis of facts, rather than on semantics. Copying of data, for example, constitutes data collection, whether or not the original source remains in place.[108] In other words, not all claims that arise from private law, such as contractual agreements or property law are relevant for the scope of the right to respect for private life.

[106] ECtHR 7 July 2015, no. 28005/12 (*M.N. and others/San Marino*), par. 51.

[107] ECtHR 24 August 1998, no. 23618/94 (*Lambert/France*), par. 21; ECtHR 25 June 2013, no. 18540/04 (*Valentino Acatrinei/Romania*), par. 53; ECtHR 2 September 2010, no. 35623/05 (*Uzun/Turkey*), par. 49.

[108] ECtHR 7 July 2015, no. 28005/12 (*M.N. and others/San Marino*), par. 54. In the *Segerstedt-Wiberg and others/Sweden*-case the ECtHR combines these aspects and found that 'the information about the applicants that was stored on the Security Police register and was released to them clearly constituted data pertaining to their *private life*. Indeed, this embraces even those parts of the information that were public, since the information had been systematically collected and stored in files held by the authorities'. The ECtHR concluded accordingly that art. 8(1) ECHR was applicable. ECtHR 6 June 2006, no. 62332/00 (*Segerstedt-Wiberg and others/Sweden*), par. 72.

2.1.1.4.2 State responsibility for actions of private entities in criminal law enforcement Private-to-public data transfers for the detection of crime raises questions on accountability. The following question arises when private entities are not confronted with an order or warrant to cooperate with criminal law enforcement authorities, but instead voluntarily help with or even initiate the partnership: To what extent is it possible to attributed the actions of private entities to the State?[109]

Only a few times the ECtHR has ruled on cases where privacy infringements were conducted by private entities while voluntarily helping the State in criminal law enforcement. In the case *A. v. France* a hitman colluded with the law enforcement authorities to build a case against his contractor.[110] In close cooperation between the hitman and the authorities, communication was intercepted during the pre-trial phase of the criminal investigation. This included the interception of a phone call in which the hitman and the contractor discussed the details of the requested assassination.[111] This wiretap interfered with the right to privacy of the contractor.[112] The French State pointed to the hitman. The State argued that the fact that the government had provided resources, such as premises and equipment, and had not opposed to the cooperation plan as such, is not sufficient to render the State responsible for the interference.[113] The Court observed that the actions of the private actor and the public authority could hardly be dissociated from each other. The hitman played a decisive role in conceiving and executing the plan to make recordings of the telephone conversations. He went to the police and called his contractor on a prepared tapped communication line. The public prosecutor and the police acted in the performance of their official duties and qualified as the *public authority*. The police officers made a crucial contribution to execution of the scheme by offering their office space, their telephone and their tape recorder.[114] The ECtHR explained that for these reasons the

[109] Another interesting question that falls outside the scope of this study is: To what extent can the private entity be held accountable? This question belongs to the domain of tort law and the horizontal effect of fundamental rights, and falls outside the scope of this study. See [Voigt and von dem Bussche, 2017] for an analysis of the tasks and powers of the supervisory authorities, civil liability, administrative sanctions, and the available judicial remedies under the GDPR. With regard to the security obligations of the data controller and tort law see: [Wolters, 2017].

[110] ECtHR 23 November 1993, no. 14838/89 (*A./France*).

[111] ECtHR 23 November 1993, no. 14838/89 (*A./France*), par. 8.

[112] ECtHR 23 November 1993, no. 14838/89 *A./France*), par. 37.

[113] ECtHR 23 November 1993, no. 14838/89 (*A./France*), par. 34.

[114] ECtHR 23 November 1993, no. 14838/89 (*A./France*), par. 35-36.

public authorities were involved to such an extent that the state's responsibility under the Convention was engaged and the interference with the rights protected under art. 8(1) could be contributed to the state.[115]

The ECtHR repeats this type of test in later cases, like the *M.M. v. the Netherlands*-case, where the actions of a private entity in the pre-trial phase of an investigation lead to accountability for the State because of the close collaboration between the private actor and the law enforcement authorities.[116] Just like the *A. v. France* case, this case was characterized by the police setting up a private individual to collect evidence in a criminal case. The Government tried to persuade the ECtHR that it was ultimately the private actor that was in control of the events. This was rejected by the ECtHR because to "accept such an argument would be tantamount to allowing investigating authorities to evade their responsibilities under the Convention by the use of private agents".[117] The ECtHR deemed it not necessary to consider that the private entity would have been fully entitled to record telephone calls from the applicant without the involvement of the public authority and use the recordings as she wished, because the issue in this case is "precisely the involvement of public authority".[118]

Another case from the Netherlands featured the use of private actors in a fact-finding inquiry for law enforcement purposes as well.[119] This case concerned a durable cooperation between a law enforcement authority and a private actor who made recordings for evidence purposes. The technical recording equipment was made available for this purpose by the law enforcement authority. The private actor used the recording also for his own purposes. The ECtHR was of the opinion that the collecting by the authority – for the purposes of an officially commissioned fact-finding inquiry – of recordings of conversations between the applicant and the private actor

[115] ECtHR 23 November 1993, no. 14838/89 (*A./France*), par. 36.

[116] ECtHR 8 April 2003, no. 39339/98 (*M.M./the Netherlands*); See also ECtHR 2 December 2014, no. 3082/06 (*Taraneks/Latvia*), par. 85: Regarding the legal basis for the recording of the applicant's conversations, the conclusion of the Senate of the Supreme Court that O.V. and S.Z. had recorded them in their private capacity are difficult to share because the police were not only well aware that the conversations were going to be recorded but they had also provided the technical equipment for that purpose and any suggestion of a legal basis that refers to them being made by O.V. and S.Z. acting in their private capacity is misguided; And more general on covert operations and privacy interference; See also ECtHR 10 March 2007, no. 4378/02 (*Bykov/Rusia*) par. 72; ECtHR 1 March 2007, no. 5935/02 (*Affaire Heglas/Republique Tcheque*), par. 71.

[117] ECtHR 8 April 2003, no. 39339/98 (*M.M./the Netherlands*), par. 40.

[118] ECtHR 8 April 2003, no. 39339/98 (*M.M./the Netherlands*), par. 41.

[119] ECtHR 25 October 2007, no. 38258/03 (*Vondel/the Netherlands*).

constituted an interference with the applicant's private life and/or correspondence which was imputable to a public authority. The ECtHR deemed it unlikely that the private actor was in control and held the government responsible for the infringement and repeated its reasoning from the *M.M./the Netherlands*-case.[120]

To summarize, in determining the accountability of the State for infringements by private entities in public-private partnerships, the ECtHR takes into account the durability of the cooperation, the contributions of the authorities, the association of the criminal law enforcement authorities with the infringing actions and the amount of control of the authorities over the actions of the private entity.

2.1.2 Charter of Fundamental Rights of the European Union

In 2009, with the entry into force of the Treaty of Lisbon, the Charter of Fundamental Rights of the European Union (CFREU) became legally binding on the EU institutions and on national governments of the Member States.[121] The Court of Justice of the European Union (CJEU) is the ultimate arbiter in the explanation of the CFREU. The following section discusses the Charter.

2.1.2.1 Scope of the Charter

The Charter addresses the institutions and bodies of the EU, including Europol,[122] and the Member States to the extent they are implementing Union law, ex art. 51(1) CFREU.[123] The criterion *implementation* has been given a wide interpretation.[124] In the 2013 the CJEU ruled on the *Åklagaren/Hans Åkerberg Fransson*-, *Melloni*-, and *Texdata Software*-case and explained that the applicability of the CFREU follows the scope of EU law because it would be undesirable to create a situation in which EU law would apply but the EU legal system would shy away from providing a fundamental

[120] The ECtHR repeated that 'to hold otherwise would be tantamount to allowing investigating authorities to evade their responsibilities under the Convention by the use of private agents'. ECtHR 25 October 2007, no. 38258/03 (*Vondel/the Netherlands*), par. 49.

[121] The Treaty of Lisbon was signed on December 13 2007 by the then 27 Heads of State or Givernment of the EU Member States. OJ C306/1.

[122] See [Hix and Høyland, 2011].

[123] The material scope of the CFREU is, therefore, less extended than the ECHR, which cover all actions of the Member States; The CJEU interprets art. 51, 52(7) CFREU and art. 6(1) TEU to define the field of application of fundamental rights in the EU.

[124] [Lenaerts, 2012].

rights protection framework within its own jurisdiction.[125] A year later the CJEU confirmed that the protection of fundamental rights in the EU is a core objective and principle of the EU and that the level of protection of fundamental rights should not vary according to national law in such a manner that it undermines the unity, primacy and effectiveness of EU law.[126] The CJEU gave a set of criteria that can be used by national courts for determining if national legislation falls within the scope of EU law: the intentions to implement EU law by the national legislature, the nature of the legislation, whether the legislation pursues objectives other than those pursued by EU law, the capabilities of the legislation to directly or indirectly affect EU law and whether there are any specific rules of EU law on the matter that are capable of affecting the national legislation.[127] The CJEU does not intend to apply the CFREU beyond the scope of the EU mandate and and does not intend to modify the powers and duties given to the European institutions in the treaties, and, therefore, the notion

[125] CJEU 26 February 2013, C-617/10, (*Åklagaren/Hans Åkerberg Fransson*), par. 21-22; CJEU 26 February 2013, C-399/11, (*Melloni*);CJEU 26 September 2013, C-418/11 (*Texdata Software*), par. 71-73.

[126] CJEU 26 April 2012, C-508/10 (*European Commission/Kingdom of the Netherlands*), par. 65: 'They may not apply national rules which are liable to jeopardize the achievement of the objectives pursued by a directive and, therefore, deprive it of its effectiveness'; CJEU 6 March 2014, C-206/13, (*Cruciano Siragusa*) par. 24-25; The increase of legislative power for the European Commission, -Council and -Parliament is counterbalanced by review of the CJEU, that had incorporated a human rights doctrine of general principles of EU law. This started long before the CFREU. See for example the *Costa/E.N.E.L.* case. CJEU 15 July 1964, C-6/64 (*Flaminio Costa/E.N.E.L.*); In 2014 the CJEU confirmed that the CFREU covers a similar scope as fundamental rights as seen as principles of EU law. E.g. CJEU 29 May 1997, C-299/95, (*Kremzow*) par. 16. CJEU 30 April 2014, C-390/12, (*Pfleger*), par. 36. In other words, the CFREU has not limited nor extended the scope of fundamental rights application in the EU. The case law shows a continuation of similar reasoning and reference to case law pre Lisbon. [Snell, 2015, p. 298]; In the mean time the doctrine of fundamental rights as principles of EU law did not cease to exist. According to art. 6(3) TEU fundamental rights, as guaranteed by the European Convention for the Protection of Human Rights and Fundamental Freedoms and as they result from the constitutional traditions common to the Member States, constitute general principles of the Union's law. The CJEU refers to the status of the right to protection of personal data and the right to respect for private life as general principles of EU is almost every ruling. E.g. CJEU 6 March 2001, C-274/99, (*Connolly/Commission*), par. 37; CJEU 20 May 2003, joined cases C-465/00, C-138/01, C-139/01, (*Rechnungshof/Österreichischer Rundfunk and Others, and Christa Neukomm and Joseph Lauermann/Österreichischer Rundfunk*), par. 68-69; CJEU 13 May 2014, C-131/12, (*Google Spain SL, Google Inc./AEPD, Mario Costeja González*), par. 68.

[127] CJEU 6 March 2014, C-206/13, (*Cruciano Siragusa*) par. 24-25. In some cases the CJEU does not apply these factors itself, which leads to problematic cases. See for example the *Willems*-case that is discussed in Section 5.1.2.2.1 on page 139.

of conferral[128] should always be taken into account.[129]

2.1.2.2 The interplay of the Charter and other sources of law

The coming into force of the Treaty of Lisbon accelerated three changes in the field of European data protection law. First of all, an independent fundamental right to the protection of personal data is acknowledged in art. 8 CFREU, which exists alongside the right to respect for private life, that is guaranteed by art. 7 of the CFREU.[130] Secondly, the role of the CJEU – the highest Court of the EU – changed. According to settled case law fundamental rights form an integral part of the general principles of EU law whose observance the CJEU ensures,[131] but only after the coming into force of the Lisbon package this role of oversight on the protection of fundamental rights is explicitly codified in the mandate of the CJEU.[132] Thirdly, data protection in the context of criminal law enforcement is now also under the jurisdiction of the EU legislature.[133]

The scope and substance of the rights protected in the Charter are determined by the text of the provisions, the intentions of the Member States in the drafting process of the Treaties and the interpretation of this by the CJEU. For the interpretation of the rights in the Charter the CJEU takes into account multiple sources of inspiration and traditions, including secondary EU law, the CJEU's body of case law, the constitutional traditions common to the Member States and guidelines supplied by international treaties for the protection of human rights on which the Member States

[128] This fundamental principle of EU law has been laid down in art. 5 TEU. It regulates that the EU may act only within the limits of the competences that EU Member States have agreed to in art. 2 to 6 TFEU. Competences not conferred on the EU by the TFEU and TEU remain with the EU Member States.

[129] CJEU 26 February 2013, C-617/10, (*Åklagaren/Hans Åkerberg Fransson*), par. 28.

[130] The two rights are closely connected. See for example CJEU 19 November 2010, C-92/09 and C-93/09, (*Volker and Markus Schecke and Eifert*) par. 47. However, over time the right to protection of personal data is transformed into a concept that is much larger than just a small cog in the wheel of privacy protection and developed into a doctrine of its own. For further reading on this topic see [Fuster, 2014a, p. 265].

[131] See CJEU 18 June 1991, C-260/89, *Elliniki Radiophonia Tiléorassi AE and Panellinia Omospondia Syllogon Prossopikou/Dimotiki Etairia Pliroforissis and Sotirios Kouvelas and Nicolaos Avdellas and others.*) par. 41; CJEU 20 May 2003, joined cases C-465/00, C-138/01, C-139/01, (*Rechnungshof/Österreichischer Rundfunk and Others, and Christa Neukomm and Joseph Lauermann/Österreichischer Rundfunk*), par.68-69; CJEU 6 March 2001, C-274/99, (*Connolly/Commission*), par. 37.

[132] Article 6 TEU.

[133] Article 16(2) TFEU.

have collaborated or to which they are signatories.[134]

When it comes to guidelines supplied by international treaties, the ECHR and the case law of the ECtHR have special significance. Article 52(3) CFREU lays down the guarantee that, in so far as the CFREU contains rights which correspond to rights guaranteed by the ECHR, the meaning and scope of those rights shall be the same or more extensive as those that have been laid down by the ECHR.[135] The CJEU follows the dynamic approach of the protection of fundamental rights of the ECtHR.[136] Over the years the CJEU has made many references to the Strasbourg case law,[137] but lately these have been declining because over the years the CJEU has built an impressive body of referable case law on fundamental rights of its own, including cases that concern data protection aspects. This body has become the Luxembourg Court's primary source of reference.[138]

2.1.2.3 Article 7 CFREU

Article 7 CFREU reads:

> *Everyone has the right to respect for his or her private and family life, home and communications*.

This provision is almost a point-to-point duplicate of art. 8(1) ECHR. The Explanatory Report of the Charter sets out that the term 'correspondence' from art. 8 ECHR is replaced by the term 'communication' to emphasise the broad scope of protection

[134] Article 6(2) and (2) TEU; Art. 52(4) CFREU; the preamble of the CFREU; CJEU 6 March 2001, C-274/99 (*Connolly/Commission*) par. 37; CJEU 18 June 1991, C-260/89, *Elliniki Radiophonia Tiléorassi AE and Panellinia Omospondia Syllogon Prossopikou/Dimotiki Etairia Pliroforissis and Sotirios Kouvelas and Nicolaos Avdellas and others.*) par. 41.

[135] See [Kokott and Sobotta, 2013] and [Ballaschk, 2015, p. 28].

[136] See J. Gerards and H. Senden on this topic. [Gerards and Senden, 2009].

[137] See for example CJEU 20 May 2003, joined cases C-465/00, C-138/01, C-139/01 (*Rechnungshof/Österreichischer Rundfunk and Others, and Christa Neukomm and Joseph Lauermann/Österreichischer Rundfunk*), par. 72; and. CJEU 24 November 2011, C-468/10 and C-469/10, (*ASNEF and FECEMD*) par. 42.

[138] See for example CJEU 24 November 2011, C-468/10, (*ASNEF*), par. 42; In case a field falls outside the jurisdiction of the EU, CJEU refers to the case law of the ECtHR without ruling on the matter. See for example CJEU 16 april 2015, C-446/12, C-447/12, C-448/12, C-449/12, (*W. P. Willems/Burgemeester van Nuth, H. J. Kooistra/Burgemeester van Skarsterlân, M. Roest/Burgemeester van Amsterdam, L. J. A. van Luijk/Burgemeester van Den Haag*).

and to take account of developments in technology.[139] Pursuant to art. 52(3) CFREU the scope of protection of art. 7 CFREU is at least similar to the scope of protection guaranteed by article 8 ECHR.[140] Comparable to the scope of art. 8(1) ECHR, the application of art. 7 CFREU is, for example, not dependent on whether the information that is communicated is of a sensitive character or whether the persons concerned have been inconvenienced in any way.[141] Limitations on art. 7 CFREU are subject to art. 52(1) CFREU, that lays down that all restriction should pursue a legitimate aim and meet the criteria of legality and proportionality, which have roots in the ECHR and the case law of the ECtHR. Limitations must also respect the essence of the right, which is a relatively new criterion that finds its inspiration in the constitutional traditions of some of the Member States.[142] These criteria will be discussed in light of the purpose limitation principle in Section 4.2 and 5.2.2.3.

2.1.2.4 Article 8 CFREU

Article 8 CFREU reads:

> *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.*

[139] Explanations Relating to the Charter of Fundamental Rights (2007/C 303/02) Explanations Relating to the Charter of Fundamental Rights (2007/C 303/02).

[140] In light of this research, this means that data is protected by the right as laid down in art. 7 CFREU, when it qualifies as data relating to private life within the meaning of art. 8 ECHR. In the data-driven society the use of big data in, for example, administrative decision making process can result in the processing of data relating to private life without qualifying as personal data. Instead of deleting personal data when the data is not necessary to serve the processing purposes anymore, controllers will increasingly anonymize data and re-use the data for other purposes. The re-use of data – for example for profiling purposes – can interfere with the right to respect for private life, when, for example, the result of data mining is used to support administrative policy decisions that interfere with the rights and freedoms of the individual. See [Koot, 2012] and [Sweeney, 2002] for an analysis of anonymity in large data sets.

[141] CJEU 8 April 2014, C-293/12 and C-594/12, (*Digital Rights Ireland*), par. 33; CJEU 20 May 2003, joined cases C-465/00, C-138/01, C-139/01, (*Rechnungshof/Österreichischer Rundfunk and Others, and Christa Neukomm and Joseph Lauermann/Österreichischer Rundfunk*), par. 75.

[142] [Brkan, 2017].

> *3. Compliance with these rules shall be subject to control by an independent authority*.

This relatively new fundamental right has a rich foundation in the existing substantive legal framework. The explanatory report of art. 8 CFREU explains that it is based on art. 16 TFEU, art. 39 TEU, Directive 95/46/EC – also known as the Data Protection Directive (DPD), the precursor of the GDPR[143] – the Data Protection Convention,[144] and art. 8 ECHR.[145] Much of the underlying ideas that are formulated in art. 8(2) and (3) CFREU have been codified in secondary EU law on data protection since the mid nineties.[146] The relationship between the Charter and secondary EU law is complex and remains a recurrent topic of debate for legal scholars.[147] On the one hand, norms from secondary data protection law have been used by the CJEU to substantiate the legal norms of art. 7 and 8 CFREU,[148] while, on the other hand, secondary data protection law has been tested against these fundamental rights norms.[149] Nevertheless, with the coming of age of the Charter and coming into force of the GDPR these issues seem less of a problem.

What remains important but somewhat unclear – even ten years after adoption of the Charter – is the relationship between the different clauses of art. 8 CFREU.[150] In

[143] See Section 2.2.2.1.

[144] See Section 2.2.1.1 on the Data Protection Convention

[145] Explanations Relating to the Charter of Fundamental Rights (2007/C 303/02);From the sources set forth in the preamble of the Charter for the purpose of identification of the rights and freedoms, only the mention of the case law of the ECtHR and the CJEU, and the common constitutional traditions of the Member States are missing from the explanation in the explanatory report. [Fuster, 2014b, p. 214].

[146] First this was codified in art. 6, 7, 12, 14 and 28 of the DPD. CJEU 8 April 2014, joined cases C-293/12, C-594/12, (*Digital Rights Ireland Ltd/Ireland, and Kärntner Landesregierung/Michael Seitlinger, Christof Tschohl and others*), par. 69; Later these provision were replaced by art. 5, 6, 15, 16 and 51 of the GDPR and with regard to processing of personal data by competent authorities for criminal law enforcement and public security purposes by art. 4, 8, 14, 16 and 41 LED.

[147] See for example [Fuster, 2014b] and [Oostveen and Irion, 2018].

[148] See for example CJEU 15 May 2011, C-543/09, (*Deutsche Telekom AG/Germany*) par. 50.

[149] E.g. CJEU 20 May 2003, joined cases C-465/00, C-138/01, C-139/01, (*Rechnungshof/Österreichischer Rundfunk and Others, and Christa Neukomm and Joseph Lauermann/Österreichischer Rundfunk*), par. 68-69; CJEU 8 April 2014, joined cases C-293/12, C-594/12, (*Digital Rights Ireland Ltd/Ireland, and KäŁrntner Landesregierung/Michael Seitlinger, Christof Tschohl and others*); CJEU 13 May 2014, C-131/12 (*Google Spain SL, Google Inc./AEPD, Mario Costeja González*) par. 69 and CJEU 11 December 2014, C-212/13, (*Ryneš*).

[150] See for example [Fuster and Gutwirth, 2013], [Fuster, 2014b] and more recent [Oostveen and Irion, 2018].

2011 the CJEU gave the impression that the criteria and rights that are formulated in the second and third paragraph of art. 8 CFREU only come into play when the right that is formulated in first paragraph is restricted.[151] If this is the case, the scope of the fundamental right to protection of personal data would be asynchronous to secondary EU data protection law.[152] From later case law a different relationship between the first and later paragraphs of art. 8 CFREU can be distilled that results in a more synchronized scope between primary and secondary law. That reading will be used in the remainder of this study.

Article 8(1) CFREU lays down a general right to protection of personal data for the individual. This right is further specified in art. 8(2) and (3) CFREU. The third paragraph also puts forward the criterion of independent oversight. Article 8(2) CFREU specifies two data subject rights: the right of access to data and the right to rectification of data. Additionally, article 8(2) CFREU lays down three conditional criteria that address the data controller: the 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. These criteria are connected to the following data protection principles: the purpose specification requirement of the purpose limitation principle, fairness and lawfulness.

2.1.2.4.1 Right to access and rectification The right of access is necessary to enable the data subject to exercise her other rights, such as the right to rectification, but also to rights that are guaranteed in secondary data protection law, such as the right to blocking, to erasure, to object to processing, or to request damages.[153] The right to access and rectification are connected to the data protection principles of transparency, data minimization, accuracy and storage limitation. In the *Schrems*-case, the CJEU connected these data subject rights to the essence of the fundamental right to effective judicial protection, as enshrined in art. 47 CFREU, which requires everyone whose rights and freedoms guaranteed by the law of the European Union

[151] CJEU 24 November 2011, C-468/10 and C-469/10, (*ASNEF and FECEMD*) par. 42.

[152] See [Fuster and Gutwirth, 2013] who pointed to the legal effects of the different readings of the relationships of the paragraphs with one another.

[153] These data subject rights are specified in art. 15, 16 and 17 GDPR and art. 23 GDPR is applicable. CJEU 7 May 2009, C-553/07 (*Rijkeboer*), par. 51-57, 59 and 64-66; CJEU 17 July 2014, C-141/12 and C-372/12 (*YS/Minister voor Immigratie, Integratie en Asiel* and *Minister voor Immigratie, Integratie en Asiel/M and S*), par. 44.

are violated to have the right to an effective remedy before a tribunal in compliance with the conditions that have been laid down in that article. The CJEU explained that legislation not providing for any possibility for an individual to pursue legal remedies in order to have access to personal data relating to him, or to obtain the rectification or erasure of such data, does not respect the essence of the fundamental right to effective judicial protection. According to the CJEU, the very existence of effective judicial review which is designed to ensure compliance with provisions of EU law is inherent in the existence of the rule of law.[154]

2.1.2.4.2 Fairness Fairness in processing and the right to access and rectification of personal data fulfill a conditional function for effective judicial protection and illustrate that the right to protection of personal data is much more than a small cog in the wheel of privacy protection.[155] In the field of criminal law enforcement and public security the data protection principle of fair processing is considered a distinct notion of the right to a fair trial as defined in art. 47 of the Charter and art. 6 of the ECHR.[156] However, public-private partnerships for the detection of criminal offenses do not trigger the safeguards of art. 6 ECHR and art. 47 CFREU, because these only apply at a later stage in the investigation when criminal charges are brought against an individual.[157] In the pre-crime phase no charges are brought against individuals, because data is shared for the detection of crime.[158]

2.1.2.4.3 Lawfulness Besides adressing the data controller the criterion of lawful processing grounds also indirectly addresses the legislature,[159] that enacted 5 other

[154] CJEU 8 October 2015, C-362/14 (*Schrems*), par. 95.

[155] CJEU 8 October 2015, C-362/14 (*Schrems*), par. 95; CJEU 1 October 2015, C-201/14 (*Smaranda Bara and Others*), par. 34.

[156] Recital 26 LED.

[157] Once a charge has been filed, art. 6 ECHR also applies to the pre-trial phase. The effects of this retrospective application fall outside the scope of this study but is intriguing which could be usefully explored in further research.

[158] See also [De Busser, 2009b, p. 169]; ECtHR 4 October 2000, no. 35394/97 (*Khan/the United Kingdom*) par. 36.

[159] In secondary data protection law legitimate processing grounds are excluded from restriction ex art. 23 GDPR. See also CJEU 24 November 2011, C-468/10, (*ASNEF*), par. 35 and 52; and CJEU 20 May 2003, joined cases C-465/00, C-138/01, C-139/01, (*Rechnungshof/Österreichischer Rundfunk and Others, and Christa Neukomm and Joseph Lauermann/Österreichischer Rundfunk*), par. 100.

legal grounds in art. 6 GDPR.[160] Legal scholars have argued against the firm position of *consent* in the Charter. Some scholars would much rather see the criterion of *necessity* be incorporated in the fundamental right to protection of personal data, which is connected to all processing grounds, including consent.[161] Other scholars have questioned the true protection of consent as a processing ground in a data-driven society, because consent is often given in a rush or by (partly) automated means , which make it questionable whether consent under these circumstances can still qualify as an informed, specific and freely given indication of intentions.[162] I agree with Poullet and Rouvroy who argue that by focussing on the individual's choice in art. 8 CFREU, personal data is protected as a commodity rather than as a part of the individual.[163]

2.1.2.4.4 Purpose specification Together with the Advocate-General of the CJEU, some scholars have (implicitly) argued that the full purpose limitation principle, including the non-incompatibility requirement, is implied in art. 8(2) CFREU because purpose specification would be of no value without the restriction on the processing of personal data for incompatible purposes.[164] One of the limitations of this account is that it fails to recognize the conditional function of the purpose specification requirement that will be described in Chapter 4 of this study. I argue that the non-incompatibility requirement is not included in the fundamental right to protection of personal data ex art. 8 CFREU. This position is based on the text of art. 8(2) CFREU and the post-Lisbon case law of the CJEU concerning re-use of personal data. As will be discussed in Section 5.1.2.2 on page 139, the CJEU consistently prioritizes the discussion of other data protection principles over the discussion of derogations from the non-incompatibility requirement. In my opinion this prioritization indicates that the non-incompatibility requirement is not part of the fundamental right to protection of personal data. The purpose specification requirement is included in the fundamental right to protection of personal data, and will be brought in relation with the essence

[160] In many instances, particularly in the surveillance situations, other processing grounds than *consent* are used.

[161] See for example [Gutwirth et al., 2009, p. 2]; The connection of necessity and consent is discussed in Section 3.5.2. See Section 4.1.2 and Section 4.1.3.4 on necessity and consent in relation to the purpose specification requirement.

[162] See for example [Poullet and Rouvroy, 2009, 45-76]; See Section 3.5.2.

[163] [Poullet and Rouvroy, 2009, 45-76].

[164] Opinion A-G, CJEU 18 July 2007, C-275/06 (*Productores de Música de España (Promusicae)/Telefónica de España SAU*), par. 53; See for example [Zarsky, 2016, p. 1006]; [Jasserand, 2018, p. 155 and 159].

of that right in Section 4.2.4 of this study.

2.1.2.4.5 Independent oversight Article 8(3) CFREU lays down the criterion of independent oversight. This provision implicitly directs the legislature to take affirmative action and adopt a framework that makes personal data processing subject to control by an independent authority.[165] The existence and independence of data protection supervisors are furthermore guaranteed in other sources of primary EU law[166] and its necessity is repeatedly underscored by the CJEU in the case law.[167]

The fundamental right to protection of personal data is not an absolute right and must be considered in relation to its function in society.[168] Restriction of this right must, however, be interpreted in light of the fundamental rights guaranteed by the Charter.[169] Similar to restrictions of art. 7 CFREU, limitations on art. 8(1) CFREU are subject to art. 52(1) CFREU, which lays down that all restriction should pursue a legitimate aim, meet the criteria of legality and proportionality and respect the essence of the right.[170]

[165] Independent oversight is also guaranteed in art. 51 and 52 GDPR and not selected for restriction ex art. 23 GDPR. The mode of operation of the supervisor can, nevertheless, differ in different contexts. In Section 5.2.2.3.2 the different types of oversight in case of secret surveillance are discussed in light of the case law of the ECtHR.

[166] Article 16(2) of the Treaty on the Functioning of the EU.

[167] CJEU 9 March 2010, C-518/07 (*European Commission/Federal Republic of Germany*). The CJEU does not refer to the Charter in this ruling; CJEU 16 October 2012, C-614/10 (*European Commission/Austria*); and CJEU 8 April 2014, C-288/12 (*European Commission/Hungary*).

[168] Recital 4 GDPR; CJEU 19 November 2010, C-92/09 and C-93/09, (*Volker and Markus Schecke and Eifert*), par.48; The CJEU builds on the framework of the ECtHR. CJEU 12 June 2003, C-112/00, (*Eugen Schmidberger, Internationale Transporte und Planzüge*), par. 80.

[169] This is similar to the restrictions on art. 7 CFREU. CJEU 20 May 2003, joined cases C-465/00, C-138/01, C-139/01, (*Rechnungshof/Österreichischer Rundfunk and Others, and Christa Neukomm and Joseph Lauermann/Österreichischer Rundfunk*), par. 68; CJEU 13 May 2014, C-131/12, (*Google Spain SL, Google Inc./AEPD, Mario Costeja González*), par. 86; CJEU 8 October 2015, C-362/14 (*Schrems*), par. 38; CJEU 21 December 2016, C-203/15 and C-698/15 (*Tele2 Sverige/Post- och telestyrelsen* and *Secretary of State for the Home Department/Tom Watson, Peter Brice, Geoffrey Lewis*), par. 91.

[170] These aspects will be discussed in light of the purpose limitation principle in Section 4.2, 4.2.4, and 5.2.2.3.

2.1.2.5 The right to respect for private life with regard to the processing of personal data

The CJEU derived from art. 7 and art. 8(1) CFREU *the right to respect for private life with regard to the processing of personal data*.[171] This *tandem right* protects the processing of data that qualifies both as *data relating to private life* ex art. 7 and 52(3) CFREU and art. 8(1) ECHR and as *personal data processing* ex art. 8(1) CFREU.[172] The CJEU applies this right frequently, but not necessarily consistently and sometimes the CJEU puts a lot of detail in the argumentation of the interference with the right protected under art. 7 CFREU, but almost skates over the interference with the right to protection of personal data.[173]

In general, the case law of the CJEU shows an ambitious – but far from finished – framework to guide in the scope of the right to respect for private life with regard to the processing of personal data.[174] The earliest judgements show teething troubles in positioning the Charter in the international and supranational legal framework, as well as in positioning art. 7 and 8 CFREU in relation to each other.[175] Later cases show

[171] See the first ruling in the field of data protection after the Charter entered into legally binding force: CJEU 19 November 2010, C-92/09 and C-93/09, (*Volker and Markus Schecke and Eifert*) par. 52; CJEU 24 November 2011, C-468/10, (*ASNEF*). In some cases the CJEU only dealt with the right to protection of personal data. See for example CJEU 15 May 2011, C-543/09, (*Deutsche Telekom AG/Germany*).

[172] Personal data can be processed without amounting to an interference with the right to respect for private life, as will be illustrated with the *Malone* and *P.G. and J.H.*-case on page 146. Similarly, data can relate to private life without qualifying as personal data, for example, the general profiles that were discussed on page 9.

[173] In the *Digital Rights Ireland*-case, for example, the CJEU only stated that the disputed measure "provides for the processing of personal data" and that it, therefore, interfered with the right protected in art. 8 CFREU. CJEU 8 April 2014, joined cases C-293/12, C-594/12, (*Digital Rights Ireland Ltd/Ireland, and Kärntner Landesregierung/Michael Seitlinger, Christof Tschohl and others*), par. 36.

[174] See [Fuster, 2014b] for a critique on the 'sloppiness' of the CJEU in the apraissal of art. 7 and 8 CFREU.

[175] With the benefit of hindsight we can now acknowledge that, for example, the reasoning in the *Schecke*-case shows multiple inconsistencies with the larger fundamental rights framework of the EU. In the *Schecke*-case the CJEU stated that the right to respect for private life with regard to the processing of personal data, recognized by art. 7 and 8 CFREU, concerns any information relating to an identified or identifiable individual. That statement appears to be misleading, when taking into account later judgements that position the 'tandem' right as a subset of personal data and a subset of data relating to private life. In the *Schecke*-case the CJEU also stated that limitations which may lawfully be imposed on *the right to the protection of personal data* correspond to those tolerated in relation to art. 8 ECHR. To this defense, art. 8 CFREU is indeed based on art 8 ECHR, but as we saw in Section 2.1.2.4, the sources for the inter-

a different and more balanced approach, in which the CJEU uses definitions from secondary data protection legislation to affirm the applicability of art. 8 CFREU, the case law of the ECtHR and the concept of *data relating to private life* to interpret the scope of art. 7 CFREU. This line of reasoning can be recognized in the *Digital Rights Ireland*-case for example. In that case the CJEU referenced the *Leander*-, *Rotaru*- and *Weber and Saravia*-case of the ECtHR, and explained that the retention of data for the purpose of possible access by the competent authorities directly and specifically affects private life and, consequently, the rights guaranteed by art. 7 CFREU.[176] The CJEU adds that such data retention also falls under the scope of art. 8 CFREU because it constitutes the processing of personal data and, therefore, necessarily has to satisfy the data protection requirements arising from the second and third paragraph of that provision.[177]

2.2 Data protection framework

In 1980 the Organization for Economic Co-operation and Development (OECD) recommended Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (OECD Guidelines).[178] These Guidelines were non-binding, but have

pretation of this right are many more. Strict interpretation of the *Schecke*-case would result in the outcome in which personal data processing instantly amounts to an interference of art. 8 ECHR, which would be in contrast with the ECtHR's case law on data processing. CJEU 19 November 2010, C-92/09 and C-93/09, (*Volker and Markus Schecke and Eifert*) par. 52.

[176] CJEU 8 April 2014, joined cases C-293/12, C-594/12, (*Digital Rights Ireland Ltd/Ireland, and Kärntner Landesregierung/Michael Seitlinger, Christof Tschohl and others*), par. 29-35.

[177] CJEU 8 April 2014, C-293/12 and C-594/12, (*Digital Rights Ireland*) par. 36; See also the *Schwarz*-case. Here the CJEU referred to the *S. and Marper*-case of the ECtHR and the definitions of personal data processing from the Data Protection Directive to explain that the storing of fingerprints qualifies as *personal data processing* because the data objectively contains unique information about individuals which allows those individuals to be identified with precision. The CJEU concludes that the taking and storing of fingerprints by the national authorities constitutes a threat to the rights to respect for private life and the protection of personal data. CJEU 10 October 2013, C-291/12 (*Michael Schwarz/Stadt Bochum*) par. 27 and 30.

[178] The OECD is a forum where Western developed counties and the European Commission work together to address economic, social and environmental challenges of globalization; The Guidelines were adopted at a critical moment in time because some member states had just adopted a national data protection act, and others were in process of drafting such a bill. In addition to this, the CoE was working on the DPC at the same moment in time. See Section 2.2.1.1. The Guidelines were revised in 2013 which was also a critical moment in time, because in that year the DPC, the DPD and the LED were on the slab too.

set the minimum standard for national, international and supranational data protection policy. They secured that the purposes for which personal data is collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.[179] Following the OECD guidelines all data protection law includes the purpose limitation principle in Europe.[180] The following Sections describe the applicable data protection framework of the Council of Europe and the European Union for data transfers from private entities to criminal law enforcement agencies for the detection of crime.

2.2.1 Relevant Council of Europe data protection framework

Besides the EU, the Council of Europe plays an important role in the protection of fundamental rights in he processing of personal data. The next subsections describe

See Section 2.2.2.1 and Section 2.2.2.2. See [Wright et al., 2011] for a critical analysis of the text before the revision.

[179] OECD Guidelines Governing The Protection Of Privacy And Transborder Flows Of Personal Data 2013, art. 3. and art. 5(b); Thirty years after the OECD Privacy Guidelines, OECD Report 2011, p. 17, 22, 23 and 70; Explanatory Notes 2013 OECD Guidelines Governing The Protection Of Privacy And Transborder Flows Of Personal Data, p. 55. Besides the guidelines the OECD made the following recommendations and declarations relating to data protection: OECD recommendation on Cross-Border Privacy Law Enforcement Co-operation; Ministerial Declaration on the Protection of Privacy on Global Networks [Annex 1 to C(98)177]; Recommendation of the Council concerning Guidelines for the Security of Information Systems and Networks [C(2002)131/FINAL]; Recommendation of the Council on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy [C(2007)67]; Declaration for the Future of the Internet Economy (The Seoul Declaration) [C(2008)99]; Recommendation of the Council on Principles for Internet Policy Making [C(2011)154]; Recommendation of the Council on the Protection of Children Online [C(2011)155]; Recommendation of the Council on Regulatory Policy and Governance [C(2012)37]. These instruments do not encompass specific rules on purpose limitation.

[180] At the highest international level, the United Nations, purpose limitation is also acknowledged. Article 3(b) UN Guidelines for Regulation of Computerized Personal Data Files, 14 December 1990, Adopted by General Assembly resolution 45/95 of 14 December 1990: “The purpose which a file is to serve and its utilization in terms of that purpose should be specified, legitimate and, when it is established, receive a certain amount of publicity or be brought to the attention of the person concerned, in order to make it possible subsequently to ensure that none of the said personal data is used or disclosed, except with the consent of the person concerned, for purposes incompatible with those specified”; The General Assembly requested governments, intergovernmental- and non-governmental organizations to take the guidelines into account in their administrative regulations and legislation, and to respect them while carrying out their activities within the field of their competence.

the most important legislative achievements of the CoE in this field.

2.2.1.1 Data Protection Convention no. 108

The CoE gave birth to the first legally binding international data protection treaty and issued non-binding recommendations on the processing of personal data in the police sector at a very early stage in the development of data protection law. The Data Protection Convention (DPC), also know as Convention 108, was the first binding treaty on data protection which expanded the notion of fundamental rights protection in databases beyond the notion of a right to privacy.[181] It was signed in the year 1981. The Convention has a long list of signatory parties, that goes beyond the Council of Europe Member States.[182] The DPC has a double role in European data protection law. On the one hand, it binds the Signatory States to take necessary measures in their domestic law in order to give effect to the basic data protection principles that have been laid down in the Convention,[183] while on the other hand, it contributes in the interpretation of art. 8 ECHR through application of the Convention's data protection principles in the case law of the ECtHR.[184] The Convention also served as a source of inspiration for the EU 1995 DPD, the precursor of the GDPR, and contributed to the foundation of the fundamental right to protection of personal data ex art. 8 CFREU.[185]

In terms of scope the DPC has a unique position in Europe. Article 8 ECHR protects data processing that falls within the scope of the right to respect for information relating to private life or correspondence, but the DPC is applicable to the processing of all personal data, regardless of whether the processing constitutes an interference

[181] Explanatory Report Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data no. 108, par. 19.

[182] The list is available on https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/108/signatures. Lastly retrieved 22 December 2019.

[183] Article 4(1) DPC; Explanatory Report of Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data no. 108, par. 18, 20 and 40; Former President of the ECtHR Ryssdal, described the Data Protection Convention as a sectoral approach of art. 8 ECHR in the context of automated data processing. [Ryssdal, 1991]; The DPC can help to interpret the obligations of the Member States of the CoE with regard to safeguarding the rights and freedoms protected in the ECHR, but the concepts of the latter enjoy 'a status of semantic independence'. [Letsas, 2004, p. 282].

[184] See for example: ECtHR 4 December 2008, no.130562/04 and 30566/04 (*S. and Marper/the United Kingdom*) par. 68 and 75; See also ECtHR 25 February 1997, no. 22009/93 (*Z/Finland*); ECtHR 16 February 2000, no. 27798/95 (*Amann/Switzerland*); ECtHR 4 May 2000, no. 28341/95 (*Rotaru/Romania*).

[185] See Section 2.1.2.4 on page 38.

with the rights protected under art. 8 ECHR.[186] The data protection instruments of the EU depend on the jurisdiction of the EU, meaning that, for example, data processing in the context of national security is excluded from their scope. This is not the case with the DPC which applies to all public and private sectors of the Signatory States. Due to its wide scope and broad ratification the Convention was also considered the standard for data protection in the field of criminal law enforcement in EU Member States prior to the adoption of the LED.[187]

The DPC was updated in 2016 in order to address privacy challenges resulting from the use of new information and communication technologies, and to strengthen the convention's follow-up mechanism on data protection interferences.[188] This study uses the new text of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data as it will be amended by the Protocol CETS No. 223.

2.2.1.2 Recommendation (87) 15 on Regulating the Use of Personal Data in the Police Sector

A few years after the adoption of the DPC the Council of Europe issued the Recommendation on Regulating the Use of Personal Data in the Police Sector in 1987.[189] This Recommendation serves as a *lex specialis* for data processing for police purposes.[190] It is non-binding in nature, but gained importance through reference by the ECtHR in their case law on data processing for police purposes.[191] The text of the Recommendation gives guidance on what can be considered a specific and legitimate purpose and explains what type of restrictions should be allowed on the data protection principles, including the purpose limitation principle that is secured in art. 5(4)(b) DPC.[192] That provision lays down that personal data undergoing process-

[186] Article 2(a) DPC.

[187] [De Busser, 2009b, p. 170].

[188] The revision process was started in 2013. See https://www.coe.int/en/web/portal/28-january-data-protection-day-factsheet. Lastly retrieved 22 December 2019.

[189] The Recommendation (87) 15 on Regulating the Use of Personal Data in the Police Sector.

[190] [Cannataci et al., 2006a] in [Cannataci et al., 2006b].

[191] E.g. ECtHR 4 December 2008, no.130562/04 30566/04 (*S. and Marper/the United Kingdom*) par. 103. and ECtHR 13 November 2012, no. 24029/07 (*M.M./the United Kingdom*) par. 196.

[192] Principle 2.1 R(87) 15: The collection of personal data for police purposes should be limited to such as is necessary for the prevention of a real danger or the suppression of a specific criminal offense. Any exception to this provision should be the subject of specific national legislation; Explanatory Memorandum

ing shall be collected for explicit, specified and legitimate purposes and not processed in a way incompatible with those purposes. This consideration of the purpose limitation principle in this Recommendation for was seen a "hallmark achievement" and "significant victory" for privacy in the late eighties.[193]

2.2.2 Relevant European Union data protection framework

The relevant EU data protection law for this study is the General Data Protection Regulation (GDPR) and the Directive (EU) 2016/680, also known as the Data Protection Directive for Police and Criminal Justice Authorities (LED). Both instruments secure the purpose limitation principle in a provision that safeguards that:

> *Personal data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.*[194]

Chapter 4 and Chapter 5 dive into the functioning of the principle in the various legal instruments. The following section introduces the legal instruments briefly and discusses their interrelationship.

2.2.2.1 General Data Protection Regulation

The GDPR replaced the 1995 DPD.[195] The legislative process for a new data protection package in the EU started in 2012 and finished in 2016 with the adoption of the

CoE R(87) 15, par. 43; The Explanatory Memorandum of stresses that all processing purposes have to be defined in the light of the interest at stake for society. Explanatory Memorandum CoE R(87) 15, par. 20 and 22; Data processing in the police sector cover all tasks which the police authorities must perform for the prevention and suppression of criminal offenses and the maintenance of public order. Appendix to Recommendation (87) 15 Scope and Definitions, line 3; Explanatory Memorandum CoE R(87) 15, par. 36.

[193] Report: Recommendation R(87) 15 Twenty-five years down the Line, CoE J.A. Cannataci en M.M. Caruana, p. 5 and 18; See Section 5.5.4 where I argue that art. 4(2) LED changes the default use limitation in the LED from compatibility of purposes to justifiability under fundamental rights criteria. This different default was already possible with the explanation of CoE R(87) 15 which was published almost 30 years prior to the LED.

[194] Article 5(1)(b) GDPR, art. 4(1)(b) LED.

[195] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal L 281 , 23/11/1995 P. 0031 - 0050.

GDPR and the LED, which is discussed in Section 2.2.2.2.[196] The Regulation follows the scope of EU law and applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.[197]

Data processing that is related to three types of activities is excluded from the application scope. Firstly, the Regulation does not apply to the processing of personal data by a natural person in the course of a purely personal or household activity with no connection to a professional or commercial activity.[198] Secondly, the GDPR does not apply to the processing of personal data by the Member States when carrying out activities in relation to the common foreign and security policy of the EU.[199] Thirdly, the Regulation excludes from its scope data processing by competent authorities for the objectives of the prevention, investigation, detection or prosecution of criminal offenses or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security and the free movement of such data.[200] Data processing in relation to these objectives is the subject of the LED. Also excluded from the scope is data processing by the Union institutions, bodies, offices and agencies.[201]

In order to trigger the territorial applicability of the GDPR, personal data should be processed within the material scope of the GDPR by a data controller who has a connection through international law ex art. 3(3) GDPR with the European Union, or by a data controller or processor who has a geo-locational connection with the European Union. This geo-locational connection can be established in three ways:

[196] The revisal was announced in the first month of the research for this study, while I visited my first international privacy conference.

[197] Article 2(1) and (2)(a), recital 16 GDPR.

[198] Article 2(2)(c) GDPR; In the *Ryneš*-case personal or household activity is determined on the basis of location by the CJEU. CJEU 11 December 2014, C-212/13, (*Ryneš*) par. 30. This reasoning is not future proof. The data-driven society is in the cloud and in a semi public/private space. Personal activities can, therefore, take place outside the house too. I agree with the CJEU that the Date Protection Directive applied, but for different reasons: the purposes for which the data was collected were not purely personal because the footage was intentionally collected to hand over to the law enforcement authority to serve as evidence. See to this extent also: [van der Sloot, 2015].

[199] Article 2(2)(b) GDPR.

[200] Article 2(2)(d) GDPR.

[201] Article 2(3) GDPR. Processing for by the EU is subject to Regulation (EU) 2018/1725, which falls outside the scope of this study.

1.) personal data is processed in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not ex art. 3(1) GDPR; or,

2.) personal data is processed of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union ex art. 3(2)(a) GDPR; or

3.) personal data is processed of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to the monitoring of their behavior as far as their behavior takes place within the Union ex art. 3(2)(b) GDPR.

The scope of article 3 GDPR must be interpreted in light of the objective that the legislature sought to prevent the data subject from being deprived of the protection guaranteed by the GDPR or that protection being circumvented.[202] The geo-locational link of the data controller gives a wide territorial and extraterritorial scope to the GDPR, because neither the nationality of the owner of the company that processes the data, nor the physical location of the personal data, nor the equipment – like the company hardware, terminal equipment of the end-user, or cloud servers – are a decisive factor.[203] The notion of *in the context of activities of an establishment* implies that the applicable law is not the law of the Member State where the controller is established, but where an establishment of the controller is involved in activities implying the processing of personal data.[204] It is irrelevant whether the processing is executed *by* that establishment.[205] The question of whether the data is processed in the context of activities of an establishment is closely related to the question on who should

[202] Recital 23 GDPR; CJEU 13 May 2014, C-131/12 (*Google Spain SL, Google Inc./AEPD, Mario Costeja González*), par. 54.

[203] Recital 22 GDPR; Article 29 Working Party *Opinion 8/2010 on Applicable Law*, 2010, WP 179, p. 8; When the DPD was still applicable this broad scope was already underlined by the CJEU. See for example: CJEU 1 October 2015, C-230/14, (*Weltimmo*), par. 27-33 and 44; CJEU 13 May 2014, C-131/12 (*Google Spain SL, Google Inc./AEPD, Mario Costeja González*), par. 53 and 54; and CJEU 12 July 2011, C/324 09 (*L'Oréal and others/eBay International AG and Others*), par. 62 and 63.

[204] Article 29 Working Party *Opinion 8/2010 on Applicable Law*, 2010, WP 179, p. 29.

[205] The display of the search results was considered personal data processing by the Court because

be determined the data controller. In other words: who determines the purposes and the means of the data processing?[206]

The Regulation lays down rules that balance the protection of fundamental rights and freedoms of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data.[207] The preamble assures that the Regulation respects all fundamental rights and observes the freedoms and principles recognized in the CFREU, in particular the respect for private and family life, home and communications, the protection of personal data, freedom of thought, conscience and religion, freedom of expression and information, freedom to conduct a business, the right to an effective remedy and to a fair trial, and cultural, religious and linguistic diversity, as well as the right to non-discrimination and the presumption of innocence.[208] The mechanisms allowing those different rights, freedoms and objectives to be balanced have been elaborated in the GDPR.[209] The use of concepts such as 'adequate', 'appropriate', 'reasonable' and 'necessary' imply the balancing nature of the instrument and a dynamic relationship between the data subject and data controller.[210]

2.2.2.2 Data Protection Directive on Police Matters

During the intergovernmental conference which adopted the Lisbon Treaty, the EU Member States acknowledged that specific rules on the protection of personal data and the free movement of personal data in the fields criminal law enforcement are necessary because of its specific nature.[211] This resulted in the LED, which is based on

it included the name of mister Gonález. See CJEU 13 May 2014, C-131/12 (*Google Spain SL, Google Inc./AEPD, Mario Costeja González*), par. 52.

[206] See Section 3.5 on page 79 to this extent. See also CJEU 13 May 2014, C-131/12 (*Google Spain SL, Google Inc./AEPD, Mario Costeja González*).

[207] Article1 GDPR.

[208] For example Recital 4 and 75 GDPR.

[209] CJEU 6 November 2003, C-101/01(*Bodil Lindqvist*) par. 82; CJEU 29 January 2008, C-275/06 (*Productores de Música de España (Promusicae)/Telefónica de España SAU*) par. 65; and CJEU 13 May 2014, C-131/12 (*Google Spain SL, Google Inc./AEPD, Mario Costeja González*) par. 97-99.

[210] E.g. Articles 5, 6, 24(1) of GDPR; The directly or indirectly identified or identifiable natural person to whom the personal data relates is the data subject. Article 4(1) GDPR. Section 4.1.2.1 discusses the necessity requirement of the lawful processing grounds and its relationship with the other references to necessity in the GDPR.

[211] Declaration No 21 on the protection of personal data in the fields of judicial cooperation in criminal matters and police cooperation, annexed to the final act of the intergovernmental conference which

art. 16 Treaty on the Functioning of the European Union (TFEU), art. 87(2)(a) and art. 82(1) TFEU. The LED has replaced Council Framework Decision 2008/977/JHA, on May 6 2018, which applied in the areas of judicial cooperation in criminal matters and police cooperation.[212] The scope of application of that Framework Decision was limited to the processing of personal data transmitted or made available between Member States.[213]

Personal data processing that is carried out by competent authorities under the LED should meet four criteria in order to be lawful ex art. 8(1) LED.[214] Firstly, the processing should be necessary for the performance of a task.[215] Secondly, the processing should be based on Union or Member State law.[216] Thirdly, the processing must respect the data protection principles ex art. 4 LED. Lastly, the data should be processed for the objectives set out in art. 1(1) LED: the prevention, investigation, detection or prosecution of criminal offenses or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.[217] The scope of the LED follows the EU mandate and does not apply to the processing of personal data in the course of an activity which falls outside the scope of Union law. Similarly excluded from the scope of the LED is data processing by the Union institutions, bodies, offices and agencies.[218] Personal data processing by, for example, Europol is regulated by a separate set of rules in the Europol Regulation that is specifically tailored to the needs of this organization.[219] The Directive is intended as minimum harmonization and art. 1(3) LED offers the Member States the possibility to provide higher safeguards than those established in the Directive for the protection of the rights and freedoms of the data subject with regard to the processing of

adopted the Treaty of Lisbon.

[212] Some scholars see art. 1(3) LED as an expansion of the data protection mission of the EU legislature in this provision. See for example: [Salami, 2017, p. 3]; art. 59 LED.

[213] Recital 6 LED.

[214] See Section 2.2.2.3 on page 55 on the concept of competent authority.

[215] See Section 4.1.2.1 on the role of the purpose specification requirement in determining the necessity and with that the lawfulness of processing.

[216] See Section 3.5.3 on page 84 on the characteristics of instruments that can qualify as a law.

[217] Article 1(1) and art. 2(1) LED. Art. 2(2) LED explains that the Directive applies to the processing of personal data wholly or partly by automated means, and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.

[218] See footnote [201].

[219] Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 may 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA

personal data by competent authorities.

2.2.2.3 Relationship between the GDPR and the LED

Traditionally, the police task in many European countries is twofold: On the one hand, there is law enforcement, which can be divided into the task of criminal law enforcement and the task of enforcement of public order, and on the other hand, there is the task of assisting the community. These tasks do not copy one-on-one to the two application fields of art. 1(1) LED: criminal law enforcement and safeguarding public security. Data processing for the criminal law enforcement task and the public order task translate to data processing for the objectives of prevention, investigation, detection or prosecution of criminal offenses, and safeguarding against and the prevention of threats to public security, but this is not so easy for the community assistance task. National legislatures struggle with this asymmetry. When data processing for the community assistance task does not fall under the scope of the LED, the GDPR is applicable to that data processing ex art. 2(1) GDPR and art. 9(2) LED. This could lead to a situation in which a police officer, who frequently cannot categorize her operations in one task exclusively, has to determine the applicable legal regime for every data processing operation while being on duty.

Since the proposal of the new regulatory framework the material scope of the LED has been subject to considerable debate that focusses on the moment when the regime of the GDPR stops and the LED regime begins.[220] Recital 12 LED is intended to explain the interrelationship of the two instruments:

> *The activities carried out by the police or other law-enforcement authorities are focused mainly on the prevention, investigation, detection or prosecution of criminal offenses, including police activities without prior knowledge if an incident is a criminal offence or not. Such activities can also include the exercise of authority by taking coercive measures such as police activities at demonstrations, major sporting events and riots. Member States may entrust competent authorities with other tasks which are not necessarily carried out for the purposes of the prevention, investigation, detection or prosecution of criminal offenses, including the safeguarding against and the prevention of*

[220] See for example [Purtova, 2018] and [Jasserand, 2018].

> *threats to public security, so that the processing of personal data for those other purposes, in so far as it is within the scope of Union law, falls within the scope of Regulation (EU) 2016/679.*

The GDPR runs a counterpart Recital, no. 19:

> *The protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offenses or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security and the free movement of such data, is the subject of a specific Union legal act. This Regulation should not, therefore, apply to processing activities for those purposes. However, personal data processed by public authorities under this Regulation should, when used for those purposes, be governed by a more specific Union legal act, namely Directive (EU) 2016/680 of the European Parliament and of the Council (1). Member States may entrust competent authorities within the meaning of Directive (EU) 2016/680 with tasks which are not necessarily carried out for the purposes of the prevention, investigation, detection or prosecution of criminal offenses or the execution of criminal penalties, including the safeguarding against and prevention of threats to public security, so that the processing of personal data for those other purposes, in so far as it is within the scope of Union law, falls within the scope of this Regulation.*

The scope of LED is to a large degree determined by the interpretation of three concepts: *competent authority* ex art. 2(1) and art. 3(7) LED juncto art. 2(1)(d) GDPR, *criminal offenses* and *public security* ex art. 1(1) LED juncto art. 2(1)(d) GDPR. Pursuant to art. 3(7) LED Member States have discretion in the appointment of which entity qualifies as a *competent authority* which entity does not. Competent authorities may include not only public authorities such as the judicial authorities, the police or other law-enforcement authorities but also any other body or entity entrusted by Member State law to exercise public authority and public powers for the purposes of the LED.[221] Some Member States took up this opportunity and appointed specific private entities as competent authorities under the national implementation of the

[221] Recital 11 LED.

LED, while others have not.[222] The concept of a *criminal offense*, on the other hand, has autonomous meaning under the LED.[223] Member States have no discretion in the interpretation of that notion.

So far, the concept of *public security* has not been attributed autonomous meaning under EU law and Member States are trying to bring the police task of community assistance under this concept. The Dutch legislature, for example, argued that the enforcement of public order and community assistance fall under the concept of public security and that all three tasks are highly intertwined. In order to maintain a high level of legal certainty, the Dutch legislature brought data processing for all three police tasks under the scope of the national implementation of the LED.[224] This is a noble idea, but the question is whether this is not falsely bringing data processing under the scope of the LED where it really belongs under the scope of the GDPR. The GDPR is an EU regulation and such regulations have set material scopes ex art. 288 TFEU. Member States do not have the authority to change that even not in cases where an appeal is made to legal certainty.

[222] See for example the situation in Italy that is discussed in a blog by Stefano Fantin https://www.law.kuleuven.be/citip/blog/law-enforcement-and-personal-data-processing-in-italy-implementation-of-the-police-directive-and-the-new-data-retention-law/. Lastly retrieved 22 December 2019; In the Netherlands *Bijzondere opsporingsambtenaren* private entities that gained public qualification, can fall under the definition of *competent authority* and can process data under the Wet politiegegevens, the Dutch implementation of the LED. *Kamerstukken II*, 34 889, nr. 3, Wijziging van de Wet politiegegevens en de Wet justitiśle en strafvorderlijke gegevens ter implementatie van Europese regelgeving over de verwerking van persoonsgegevens met het oog op de voorkoming, het onderzoek, de opsporing en vervolging van strafbare feiten of de tenuitvoerlegging van straffen, Memorie van Toelichting.

[223] Recital 13 LED.

[224] *Kamerstukken II*, 34 889, nr. 3, Wijziging van de Wet politiegegevens en de Wet justitiśle en strafvorderlijke gegevens ter implementatie van Europese regelgeving over de verwerking van persoonsgegevens met het oog op de voorkoming, het onderzoek, de opsporing en vervolging van strafbare feiten of de tenuitvoerlegging van straffen, Memorie van Toelichting, par. 5.2.1.

Chapter 3

General notion of purpose limitation

This chapter seeks the answers to the subquestions that relate to role of the purpose limitation principle in data protection law. However, as the later chapters will show the role of the purpose limitation principle in data protection law cannot be determined without taking into account its role in fundamental rights law. The groundwork for the analyses in these later chapters is done here.

This chapter describes the general notion of the purpose limitation principle. The first section discusses the general idea behind the principle and is meant as an introduction on the basics of the principle. The second section zooms in on the different terminology that is used by legal scholars, the EDPB and EU legislature to talk about the ideas behind the principle or the principle itself. Section 3.3 discusses the six elements that can be found in the common definition of purpose limitation that can be found in EU data protection law. The next section, Section 3.4, elaborates on two higher goals that are associated with the principle.[225] The first goal relates to autonomy and self-determination and the second goal relates to the Rule of Law. Lastly, in Section 3.5, the position of the purpose limitation principle is investigated in relation to other key rules and principles in EU data protection law.

3.1 The function of purpose limitation

The purpose limitation principle obligates the data controller to perform two operations. Firstly, the principle demands prior transparency of intentions by specifying the purposes, and, secondly, it binds the controller to (self) pre-determined conditions by

[225] The word *goal* is chosen to make a clear distinction between the concept of *purpose* and the concept *objective* that are used in this study. See Section 3.3.1 and Section 1.2 on page 10.

limiting the use of personal data to the specified purpose.[226] Thus, we can derive two requirements: the *purpose specification*- and the *non-incompatibility requirement*.[227] Purpose limitation helps in "understanding why certain personal data is being processed'.[228] The purposes determine a chain of processing actions within one processing operation that starts at the moment of collecting the data and ends at the moment the purposes are fulfilled. The purposes specification, therefore, categorizes the data processing into viable processes with a start and end point: a processing operation.[229] In most cases the processing purposes concern the intention of the processing after the data collection phase. And as such purpose specification can cast a glance at the future. It is, nevertheless, important to take into account the societal and technological conditions at the time of the exposition of intention, when interpreting the degree to which the data controller is operating within the limits of pre-determined conditions. To this extent the purpose specification is as much a period piece as it is a letter of intent.

The purpose limitation principle prohibits unspecified data collection or data processing.[230] This prohibition includes processing for the purpose of being "better safe than sorry" or the purpose of "we never know when this will come in handy". Purpose limitation is opposite to *general purpose processing* of data that is led by the interests of the data controller.[231] Purpose limitation contributes to the process of striking a balance between on the one hand the interests of the data controller or societal interest to be guarded by the legislature, and on the other hand the interests, rights and freedoms of the data subject.[232]

[226] See for a general overview of the purpose limitation principle in the EU the EDPB report: Article 29 Working Party *Opinion on Purpose Limitation*, 2013, WP 203.

[227] See the next section for a discussion of the vocabulary that is used to describe the purpose limitation principle by various scholars.

[228] Article 29 Working Party *Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector*, 2014, WP 221, p. 16.

[229] See Section 1.3.1 on page 11 of this study.

[230] Article 29 Working Party *Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector*, 2014, WP 221, p. 16.

[231] Report: recommendation R(87) 15 Twenty-five years down the Line, CoE J.A. Cannataci en M.M. Caruana, p. 5. See Section 1.1 were I briefly discuss the idea of Prins and Moerel to replace purpose limitation with the legitimate interest of the data controller.

[232] Gellman speaks of a "self-balancing feature of purpose limitation'. [Gellman, 2002].

3.2 Terminology and definitions of purpose limitation

The theoretical foundations of the purpose limitation principle in data protection doctrine originate from Allan Westin's famous work *Privacy and Freedom* from the late sixties.[233] He reasoned that the specification of the processing purpose empowered the data subject to have control over her privacy.[234] Soon after this theoretical introduction the principle was adopted in policy reports and recommendations by, for example, the Younger Committee that was installed to report on a suitable data protection framework for the United Kingdom in the early seventies.[235] That committee formulated data protection safeguards which show the early contours of the purpose limitation principle, by recommending that personal data should be held for a specific purpose and should not be used for other purposes without appropriate authorization.[236]

Since then legal scholars have used a diverse lingo to discuss the idea of purpose limitation.[237] In the early ninetees Bennett and Gutwirth independently of each other referred to the purpose limitation principle as the *principle of finality*.[238] Cannataci has referred to purpose limitation with just the word *purpose*.[239] He also used the term *purpose specification*, that Zarsky followed.[240] Stalla-Bourdillon and Knight speak of *preserve purposes*.[241] Koops and Hildebrandt have both used *purpose bind-*

[233] [Westin, 1967].

[234] [Westin, 1967, p. 33–37 and 387] Westin approached privacy as the right to control the way others use information concerning you.

[235] Great Britain: Home Office, *Report of the Committee on Privacy*, Chair: Kenneth Younger, London: H. M. Stationery Office 1972; Sweden: Justice Department, "Data och integritet" (Data and Privacy), Stockholm SOU 1972:47, Allmänna Förl. 1972; USA: Secretary's Advisory Committee on Automated Personal Data Systems, "Records, Computers and the Rights of Citizens", Washington, D.C., Department of Health, Education, and Welfare 1973; EC-Resolution on the protection of the rights of the individual in the face of developing technical progress in the field of automatic data processing C60/48 13 March 1975.

[236] The Committee also recommended that the access to the data, should be limited to those people that are authorized for the purpose for which the data was supplied and the amount of data collected and stored should be the minimum necessary for the achievement of the specified purpose. See on this topic [Gellman, 2017, p. 4].

[237] The idea of the purpose limitation principle is described in different laws under various different terms and definitions. This will be discussed in Section 2.1 on page 21;The author is well-aware that the list that follows is not exhaustive, for it serves as an illustration.

[238] [Bennett, 1992]; [Gutwirth, 1993].

[239] [Cannataci et al., 2006a, p. 48].

[240] [Cannataci and Bonnici, 2010]; [Zarsky, 2016, p. 1008-1009].

[241] [Stalla-Bourdillon and Knight, 2018, p. 17].

ing, which is a direct translation of the Dutch word *doelbinding*.[242] The EDPB has used various terms, including *purpose limitation*.[243] *specificity principles* and *purpose diversion*.[244]

Besides this diversity in names, the explanations of the purpose limitation principle in academic literature show great diversity too. The scope of the principle appears to be suffering from what one could call a *yo-yo effect* because the principle has been interpreted in ways that include and exclude other data protection principles as components of the principle.[245] Gutwirth, for example, closely followed the Belgium privacy act of 1992, and because of the wording of those provisions he differentiated three components of purpose limitation: purpose specification, use limitation and data quality.[246] Twelve years later Cannataci delivered a very narrow interpretation by encapsulating the principle in the following questions: What is the purpose for which data is collected in the first place and what is the onward-use of such data? Is it compatible with the purposes for which the data was collected in the first place?[247]

An expanded notion of the purpose limitation principle has been derived from the DPC and the 1995 DPD by Brouwer in 2011.[248] She argued that purpose limitation includes different layers of protection. It first of all prohibits the collection of personal data for unknown or unspecified purposes, referred to by her as the "ban on aimless data collection". Secondly, it implies that the goals of data processing should be legitimate, meaning that the data processing should be in accordance with the law. Thirdly, the principle demands that the goals must be specified prior to the data collection, which is commonly referred to as purpose specification. Next, any use or disclosure of personal data for goals incompatible to the (specified) goals of the data processing must be considered as unlawful. Finally, purpose limitation implies that data may not be retained longer than necessary for the purposes for which the data

[242] [Koops, 2011]; [Hildebrandt, 2014].

[243] Article 29 Working Party *Opinion on Purpose Limitation*, 2013, WP 203.

[244] Article 29 Working Party *Opinion 3/1999 on the preservation of traffic data by internet service providers for law enforcement purposes*, 1999, WP 25; Article 29 Working Party *Opinion 3/2012 on developments in biometric technologies*, 2012, WP 193, p. 30.

[245] The conditional function of the purpose specification requirement in relation to the data protection principles is discussed in Section 4.1.3 on page 102.

[246] [Gutwirth, 1993, p. 22-23]. In light of the purpose limitation principle he explained that personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.

[247] [Cannataci et al., 2006a, p. 28].

[248] [Brouwer, 2011].

are stored. In other words, "the data controller should be bound by time limits".[249]

These different legal and conceptual definitions do not necessarily contribute to an accessible debate on the value of the purpose limitation principle. This issue was underlined by Cate in a critical article about the *fair information practice principles*[250] and their implementation in US legislation.[251] He wondered what the difference is between collection limitation, purpose specification, and use limitation, that all are part of the OECD Guidelines,[252] and how these concepts compare with purpose limitation as that term is used to describe a related concept that is centrally positioned in EU data protection law. He also asked if the latter concept includes all three of the former.[253] Cate does not answer these questions, nor do other legal scholars, but this does not take away their relevance because even the EU legislature appears to be inconsistent in the application of these concepts. In the preamble of the LED, for example, the term *principle of specificity*, pops up like a jack-in-the-box.[254] No context to this term is given and it is not repeated in the main text of the LED. Because the term *purpose limitation* is most consistently used in EU data protection law this name will be used in this study, together with the two requirements that can be derived from the principle: the *purpose specification requirement* and the *non-incompatibility requirement*.

3.3 The elements of purpose limitation

The first codifications of purpose limitation included separate provisions for the purpose specification- and non-incompatibility requirement.[255] In the modern phrasing

[249] [Brouwer, 2011, p. 277].

[250] The fair information practice principles (FIPPs) are a set of principles that represent widely accepted concepts concerning fair information practice in an electronic marketplace. These are seen as the US equivalent of the data protection principles. In short the FIPPs cover principles on notice, choice, access, security and redress. See Bennet for a discussion of the contextual difference between the FIPPs and the data protection principles. [Bennett, 1992]; See [Tene, 2013] and [Marcinkowski, 2013] on the developments in the EU and the US with regard to privacy protection in the last ten years.

[251] [Cate, 2016].

[252] See Section 2.2 of this study.

[253] [Cate, 2016, p. 355-356].

[254] Recital 71 LED.

[255] See, for example, Organization for Economic Cooperation and Development, ICCP Subcommittee, Guidelines on the Protection of Privacy and Transborder Flow of Personal Data (C(80)58/FINAL) (Sept. 23, 1980) par. 9 and 10; Recommendation 87(15) art. 2.1 and 4.

of the purpose limitation principle in EU law the two requirements can be separately identified, while being bound together at the same time:[256]

> *Personal data shall be collected for specified, explicit and legitimate purposes and not processed in a manner that is incompatible with those purposes.*[257]

Six elements of interest can be distilled from this sentence. The central element of *a purpose* relates to the full purpose limitation principle and is discussed in Section 3.3.1. The element of *legitimacy, specificity, explicitness* and the *timing* aspects relate to the purpose specification requirement that safeguards that personal data shall be collected for priorly specified, explicit and legitimate purposes. These will be discussed in Section 3.3.2 to 3.3.5. Lastly, in Section 3.3.6 the element *compatibility* is discussed, which relates to the non-incompatibility requirement demanding that personal data is not further processed in a manner that is incompatible with the specified purposes.

3.3.1 The notion of a processing purpose

A purpose is generally seen as the answer to the question "Why is data being processed?" and it is complementary to the question "How is data processed?", which gives insight into the means of processing.[258] The purposes and the means are commonly determined by the data controller.[259] In situations where the purposes and means of processing are determined by law, that same law can also point to the controller or provide the specific criteria for the nomination of the data controller.[260] A controller always has a certain interest in the processing of the personal data, which can be pinpointed by looking at the greater benefit to the data controller in relation to the objectives of the data processing. However, even in these cases the broader stakes of the data processing can be formulated at a more abstract level compared to the purpose specification that describes the interests in light of proportional processing and the circumstances of the case. The purpose specification should be suitable

[256] [p. 292][Nissenbaum, 2015].

[257] See for example art. 4(1)(b) LED, art. 28(1)(b) Europol Regulation and art. 591)(b) GDPR.

[258] Article 29 Working Party *Opinion 1/2010 on the concepts of "controller" and "processor"*, 2010, WP 169, p. 13.

[259] Article 29 Working Party *Opinion 1/2010 on the concepts of "controller" and "processor"*, 2010, WP 169; Art. 4(1)(7) GDPR, art. 3(1)(8) LED.

[260] Article 4(1)(7) GDPR, art. 3(1)(8) LED.

to form the base for other proportionality decisions, such as data minimization and storage limitation.[261]

By default the purposes must be expressed in a *purpose specification* and must be communicated to the data subject.[262] The communication of this statement can be done in multiple ways, for example by providing information to data subjects, and through legislation, administrative decrees, and licenses provided by supervisory authorities.[263] A formal reading of the processing purposes looks at the written statement to discover the explicit or implicit intentions of the data controller and will exclusively use the statement to assess the compatibility of the purposes of further processing.[264] This formal assessment can lead to a legalistic approach of data protection that might encourage data controllers to point to ambiguously formulated purpose statements in hope of ensuring a wide margin of compatible purposes for further processing. This would, however, place the data subject at a disadvantage.

Rauhofer, who studied the consolidation of over 60 privacy policies of Google Services into one comprehensive Google Privacy Policy in 2012, explains that even if "the original specified purpose permits a data controller to process two distinct sets of personal data for the same or a similar purpose [...], this does not mean that this would also authorize the combination of those two data sets for that same purpose if the impact of that further processing on the user is significant, for instance, if the data is combined and processed with other data for profiling purposes."[265] To avoid problems similar to those that arose with the Google Privacy Policy consolidation, the EDPB pointed to a substantive assessment of the purposes, that goes beyond the formal statements to identify the processing purposes and takes into account the way the

[261] See Section 4.1.3 on the dependency on the purpose specification requirement of the proportionality decision that should be made in the application of the data protection principles, which are also briefly discussed in Section 3.5.1; See Section 1.1 and 4.1.2.1 on the discussion on legitimate interests and purposes; Article 29 Working Party *Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC*, 2014, WP 217, p. 24.

[262] See for example Chapter III Section 1 of the GDPR and Chapter III of the LED. The transparency obligations of the data controller, that include the communication of the processing statement, can be restricted. This is discussed in Section 5.2.1.1 on page 153. It is important to keep in mind that the obligation to communicate the purpose can be restricted but not the obligation to specify the purposes.

[263] Explanatory Notes 2013 OECD Guidelines Governing The Protection Of Privacy And Transborder Flows Of Personal Data, par. 54.

[264] Article 29 Working Party *Opinion on Purpose Limitation*, 2013, WP 203, p. 20.

[265] [Rauhofer, 2015, p. 9].

purposes are – or should be – understood, depending on the context and other factors.[266] The EDPB regards the substantive assessments "more flexible and pragmatic, but also more effective: it may also enable adaptation to future developments within the society while at the same time continuing to effectively safeguard the protection of personal data".[267]

3.3.2 Legitimacy

The element of *legitimate purposes* refers to a substantive conception of legitimacy,[268] that reaches beyond a formal check of the validity of the lawful processing grounds.[269] The legitimacy of the processing purposes falls under the responsibility of the data controller, who has the duty to process personal data *in accordance with the law*, state of the art techniques and cultural and societal norms.[270] Section 4.2 discusses the relationship between purpose specification and the criterion *in accordance with the law* and the other criteria of art. 8(2) ECHR. The case law of the CJEU shows that in order for processing purposes to be legitimate, the interests have to be justified by a link between the data, the type of data, the data subjects or group of data subjects and the objective pursued.[271] The purposes of data processing have to be assessed in light of all fundamental rights and freedoms of the data subject, but the CJEU most

[266] Article 29 Working Party *Opinion on Purpose Limitation*, 2013, WP 203, p. 21. The Working Party discusses the formal and substantive readings of processing purposes in light of the compatibility test. I believe that this reading should be used for the assessment of purposes regardless of the type of assessment. For example, when data is being processed on the base of art. 4(2) LED for purposes that fall under the scope of the LED, the purposes should be pinpointed through a substantive assessment in order to determine if the data is truly processed for the purposes referred to in art. 1(1) LED. Further processing on the base of art. 4(2) LED is discussed in Section 5.5 on page 181.

[267] Article 29 Working Party *Opinion on Purpose Limitation*, 2013, WP 203, p. 21.

[268] On the relationship between the purpose specification requirement of the purpose limitation principle and the notion of "in accordance with the law" in human rights law protection see Section 4.2 on page 117.

[269] See Section 3.5.2 on the cumulative obligation for the data controller to base the processing on a legitimate processing ground.

[270] Article 29 Working Party *Opinion on Purpose Limitation*, 2013, WP 203, p. 20.

[271] CJEU 8 October 2015, C-362/14 (*Schrems*), par. 93; CJEU 8 April 2014, joined cases C-293/12, C-594/12, (*Digital Rights Ireland Ltd/Ireland, and Kärntner Landesregierung/Michael Seitlinger, Christof Tschohl and others*), par. 57; CJEU 21 December 2016, C-203/15 and C-698/15 (*Tele2 Sverige/Post- och telestyrelsen* and *Secretary of State for the Home Department/Tom Watson, Peter Brice, Geoffrey Lewis*), par. 105.

commonly balances the rights protected in art. 7 and 8 CFREU against the interests, objectives and purposes of data processing. This is illustrated in the *Digital Rights Ireland*-case and the *Tele2*-case, that concerned a telecommunication metadata retention law for criminal law enforcement objectives. The CJEU reviewed the legitimacy of this objective in relation to the processing means and purposes, and concluded that given the seriousness of the interference with fundamental rights, only the objective of fighting *serious crime* is capable of justifying a measure that provides for telecommunication metadata, but this objective has to be defined more specifically in order to function as legitimate processing purposes.[272] In these cases the processing purposes were implicitly deemed not legitimate as well as not properly specified, due to being too general.[273]

The right to non-discrimination between EU nationals has also been balanced against the objectives of data processing in the *Huber*-case that dealt with the legitimacy of a German nation-wide database with registrations of non-German EU citizens for the purpose of determining the right of residence.[274] The data collected for this initial purpose was further processed for criminal law enforcement purposes. The personal data of German citizens was not collected in a nation-wide database and not further processed for criminal law enforcement purposes. The initial processing purposes and means of the EU residence database were considered legitimate by the CJEU,[275] but this was not the case for the secondary processing purposes. The CJEU underlined that criminal law enforcement purposes necessarily involve the prosecution of crimes and offenses committed, irrespective of the nationality of the perpetrators. The Court explained that the difference in treatment that arose by virtue of the systematic processing of personal data, relating only to Union citizens who are not nationals of the Member State for the purposes of fighting crime, constitutes prohibited discrimination.[276] For these reasons the processing purposes were considered

[272] CJEU 21 December 2016, C-203/15 and C-698/15 (*Tele2 Sverige/Post- och telestyrelsen* and *Secretary of State for the Home Department/Tom Watson, Peter Brice, Geoffrey Lewis*), par. 102; CJEU 8 April 2014, joined cases C-293/12, C-594/12, (*Digital Rights Ireland Ltd/Ireland, and Kärntner Landesregierung/Michael Seitlinger, Christof Tschohl and others*), par. 60.

[273] See on this topic also: European Human Right Cases 2017/79, M.E. Koning, *Annotation to CJEU Tele2, C 203/15 and C-698/15*; and European Human Right Cases 2014/140, M.E. Koning, *Annotation to CJEU Digital Rights Ireland, C-293/12 and C-594/12*.

[274] CJEU 16 December 2008, C-524/06, (*Huber/Germany*) par. 40.

[275] CJEU 16 December 2008, C-524/06, (*Huber/Germany*) par. 62.

[276] CJEU 16 December 2008, C-524/06, (*Huber/Germany*) par. 78-81.

not legitimate by the CJEU.

3.3.3 Specificity

The legitimate processing purposes should be identified precisely and fully in order to facilitate an average data subject, without expert legal or technical knowledge, in the assessment of what processing is and what processing is not included in the processing operation.[277] The element of specificity also enables the data controller to have an overview on her (business) case before she starts to collect data.[278] It forces the data controller to evaluate her intentions. The case law of the ECtHR on infringements of art. 8 ECHR with data protection aspects, highlights that the more a data subject is affected by the data processing, the more specified the processing purposes will have to be.[279]

In case of serious shortcomings with regard to the specificity of the purpose statement, the EDPB explains that all the facts should be taken into account to determine the actual purposes, along with the common understanding and reasonable expectations of the data subjects based on the context of the case.[280] The assessment should be based on the nature of the relationship between controller and subject, the customary and generally expected practice in the given context.[281]

There is discussion about the meaning of the specificity element. Some scholars, who focus on big data and not necessarily on big data in light of fundamental rights, argue that the element requires a 'specified' purpose and not a 'specific' purpose. To cater for data-driven and general purpose analytics, Stalla-Bourdillon and Knight, for example, contend that a 'specified purpose' should be understood as a purpose that is described with clarity and accuracy and it is, therefore, not necessarily specific in the sense of positively specifying the outcome of the processing.[282] In their eyes a nega-

[277] Article 29 Working Party *Opinion on Purpose Limitation*, 2013, WP 203, p. 39; and Article 29 Working Party *Opinion 02/2013 on apps on smart devices*, 2013, WP 202, p. 17.

[278] Article 29 Working Party *Opinion 02/2013 on apps on smart devices*, 2013, WP 202, p. 17.

[279] This is discussed in Section 5.2.2.3.2 on page 162 and Section 5.2.2.3.3 on page 167.

[280] Article 29 Working Party *Opinion on Purpose Limitation*, 2013, WP 203, p. 24-25, 39. In order to assess the reasonable expectation of privacy the outcome of the reaction of a reasonable person who is confronted with the data processing should be taken into account.

[281] Article 29 Working Party *Opinion on Purpose Limitation*, 2013, WP 203, p. 24-25, 39.

[282] [Stalla-Bourdillon and Knight, 2018, p. 10 and 17] They describe Data-driven and general purpose analytics as having "no knowledge on the type of analysis to be performed by a third party. This is the

tive description of the outcome of the processing should always be present in order to explain the consequences of the analysis.[283] They argue that a purpose of data-driven general analysis meets the specificity principle as long as it is made clear that the processing stops after the general analysis. When the data controller wants to attach consequences to the analysis, a compatibility test will have to be made.[284] Their model frames the means instead of the intended outcome of processing as central to the specificity requirement and therefore fails to produce purpose specifications that can be used in the proportionality assessments that have to be made for the application of other data protection touchstones,[285] such as the necessity assessment in the application of the legitimate processing grounds and data protection principles, like the storage limitation principle. What is more, the authors refer to the compatibility assessment of the purposes of further use with the purposes of data collection for the general analysis, but as I will argue in Section 4.1.3.3, this assessment needs specified purposes as an input in order to determine, for example, the distance between the new purposes and initial purposes. This test will not function with a negatively formulated purpose specification.

In line with the GDPR,[286] the EDPB refers to *specific purposes* in its Opinion on Purpose Limitation, when it explains that "a purpose that is vague or general [...] will – without more detail – usually not meet the criteria of being 'specific'."[287] Unspecific purposes include improving user experience, marketing purposes, IT-security purposes, future research,[288] product innovation[289] and law enforcement.[290] Pur-

usual case in which data is published through a server for future use. It also includes the case that data is transferred to a data miner or a data scientist for its analysis as we usually do not know which algorithm will be applied to the data. For this purpose, anonymization methods, also known as masking methods have been developed." It is unclear what the authors mean by *data is published through a server for future use*.

[283] As example of the negative outcome they list "no individual decisions will be adopted at the end of the analysis and the data will be destroyed". [Stalla-Bourdillon and Knight, 2018, p. 17]

[284] [Stalla-Bourdillon and Knight, 2018, p. 17]

[285] See Section 3.5 on the cumulation of data protection touchstones.

[286] Recital 39 GDPR.

[287] Article 29 Working Party *Opinion on Purpose Limitation*, 2013, WP 203., p. 16.

[288] Article 29 Working Party *Opinion on Purpose Limitation*, 2013, WP 203., p. 16.

[289] Article 29 Working Party *Opinion 02/2013 on apps on smart devices*, 2013, WP 202, p. 23.

[290] Article 29 Working Party *Opinion 03/2015 on the draft directive 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 offenses or the execution of criminal penalties, and the free movement of such data*, 2015 WP 233, p. 6.

poses like these are called *elastic purposes* and are as such inadequate to inform a data subject, supervisory authority or any other third party,[291] let alone be suitable to base proportionality decisions on, such as data minimization and storage limitation.[292]

The EU legislature does admit, however, that when it comes to scientific research, it is often not possible to fully identify the purpose at the time of data collection. This impossibility led to the only exemption in EU general data protection law with regard to the specificity requirement of the purposes. Pursuant to Recital 33 of the GDPR data subjects should be allowed to give their consent to certain areas of scientific research or parts of research projects to the extent allowed by the intended purpose when in line with recognized ethical standards for scientific research.[293]

3.3.4 Explicitness

The processing purposes should be clearly revealed, explained and exposed so that an unambiguous understanding of the processing purposes will be reached by all the

[291] Article 29 Working Party *Opinion 02/2013 on apps on smart devices*, 2013, WP 202, p. 23.

[292] See Section 4.1.3 on the dependency on the purpose specification requirement of the proportionality decision that should be made in the application of the data protection principles, which are also briefly discussed in Section 3.5.1.

[293] The purpose specification requirement is not restrictable under art. 23(1) GDPR nor under any other restriction clause in the GDPR or in other European data protection law. The scope of art. 23(1) GDPR is discussed in Section 5.2.1.1 on page 153. It is unclear if Recital 33 GDPR should be explained as: The processing for not fully identified purposes in the research field is only permitted when the processing is based on consent ex art. 6(1)(a) GDPR. Or that Recital 33 GDPR be explained as: Independent of the lawful processing grounds, the data subject will have to provide (additional) consent to the processing of personal data for not fully identified purposes in the research field. These different readings make a difference for the legitimate processing grounds for research with special categories of data, and in particular the scope of art. 9(2)(j) GDPR, which provides a processing ground that is able to lift the processing ban of art. 9(1) GDPR, that prohibits the processing of special categories of personal data. In the later explanation, research with special categories of data is possible for purposes that are not fully defined based on art. art. 9(2)(j) GDPR. The data controller will have to obtain additional consent for the data subjects where they consent to a certain level of undefinedness of the purposes. If Recital 33 should be explained as only permitting processing of personal data for not fully identified purposes in the research field on the bases of consent, research with special categories of data cannot be based on art. 9(2)(j) GDPR and instead, has to be based on art. 9(2)(a) GDPR: explicit consent. The term explicit refers to the way consent is expressed by the data subject. See Section 4.1.2.4 on page 100 on the dependency on the purpose specification requirement of the lawful processing of special categories of data.

involved parties, including the data subject, supervisory authority and other third parties. The element of *explicitness* is distinctive to the data protection framework of the EU and is missing in, for example, the Data Protection Convention of the Council of Europe[294] or the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.[295] The element was first introduced in the 1990 non-binding United Nations Guidelines for Regulation of Computerized Personal Data Files.[296] Five years later the element entered binding data protection law through the adoption of the DPD by the EU, which prescribed that Member States shall provide that personal data must be collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes.[297]

The use of covert data collection methods in the context of criminal law enforcement and the criterion of explicit purposes for data processing might appear as contradictory. The ECtHR case law underlines that restricting measures should indicate the scope of discretion conferred on the competent authorities as well as the manner of its exercise with sufficient clarity, having regard the legitimate aim of the measure in question.[298] The EU legislature tackles this contradiction in the preamble of the LED by connecting the specificity criterion to the art. 8(2) ECHR criteria. The recital explains that as long as covert methods are laid down by law and constitute a necessary and proportionate measure in a democratic society with due regard for the legitimate interests of the natural person concerned, these methods can be used for the purposes of the prevention, investigation, detection or prosecution of criminal offenses or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.[299] Section 5.2.2.3.2 on page 166 of this study discusses the set of minimum safeguards developed by the ECtHR to avoid arbitrary interferences and abuses of power in the context of secret measures of surveillance.

[294] See Section 2.2.1.1 on page 47.

[295] Thirty years after the OECD Privacy Guidelines, OECD Report 2011, p. 17, 22, 23 and 70; and Explanatory Notes 2013 OECD Guidelines Governing The Protection Of Privacy And Transborder Flows Of Personal Data, p. 55; OECD Guidelines Governing The Protection Of Privacy And Transborder Flows Of Personal Data 2013, art. 3. and art. 5(b).

[296] See Section UNguidelines on page 46.

[297] Art. 6(1)(b) DPD.

[298] ECtHR 2 Augustus 1984, no. 8691/79 (*Malone/the United Kingdom*) par. 86.

[299] Recital 26 LED.

3.3.5 Timing

The specification of the purposes *ex ante* is the yardstick in the *ex post* control and enforcement mechanisms of data protection regulation. As a general rule the specific purposes for which personal data are processed should be explicit and legitimate and determined at the time of the collection of the personal data.[300] New processing purposes can lead to a new obligation for the data controller to communicate the processing purposes to the data subject. Public authorities, for example, have to both inform the public about the databases they maintain in a general sense, and inform an individual about her data being processed in a specific case.[301]

3.3.6 Compatibility

The element of compatibility relates to the non-incompatibility requirement of the purpose limitation principle. The non-incompatibility requirement gives some flexibility to data controllers with regard to further use of personal data.[302] The compatibility element does not hint at what kind of processing should fall under further processing, it rather makes a distinction between the very first data processing, the collection of data, and al subsequent processing within that processing operation, such as storage, analysis, deletion etc.[303]

The text of the purpose limitation principle holds a double negation: personal data must be collected for specified, explicit and legitimate purposes and *not* further processed in a manner that is *incompatible* with those purposes. This type of linguistic structure is beloved by legal scholars and much hated by the rest of the world, and, learning from my experience as a teacher, particularly hated by aspiring computer scientists. The obligation not to process personal data for incompatible purposes suggests an obligation to limited review through a test of reasonability: do the initial and

[300] Recital 39 GDPR; In contrast to other data protection instruments from the same time period, the 1980 OECD guidelines are detailed on the timing of the purpose specification: before, and in an case not later than at the time of the data collection, the processing purposes must be identified. Later changes of purposes should likewise be specified. Explanatory Notes 2013 OECD Guidelines Governing The Protection Of Privacy And Transborder Flows Of Personal Data, par. 54.

[301] Committee of Ministers of the Council of Europe Resolution on the Protection of the Privacy of Individuals vis-a-vis Electronic Data Banks in the Public Sector, (74) 29, par. 1.

[302] Article 29 Working Party *Opinion on Purpose Limitation*, 2013, WP 203, p. 21.

[303] [Forgó et al., 2017, p. 29].

new purposes appear not to be incompatible? In other words: Can the data controller at this moment in time reasonably suggest that the purposes are not incompatible with each other?[304] Article 6(4) juncto Recital 50 GDPR gives the following factors that should be taken into account in such a test:

a Any link between the purposes for which the personal data have been collected and the purposes of the intended further processing.

b The context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller and including the reasonable expectations of data subjects based on their relationship with the controller as to their further use.

c The nature of the personal data, in particular whether special categories of personal data are processed, or whether personal data related to criminal convictions and offenses are processed.

d The possible consequences of the intended further processing for data subjects.

e The existence of appropriate safeguards in both the original and intended further processing, which may include encryption or pseudonymisation.

3.4 Higher goal of purpose limitation

This section describes the higher goals that are connected to the purpose limitation principle by legal scholars and the EDPB. The purpose limitation principle is connected with underlying substantive concepts that give it its weight, yet different readings exist as to the type and number of these. In all readings the purpose limitation principle is connected to concepts that support both individual and societal goals that require a dynamic approach towards transparency of data processing and opacity of the data itself.[305] The EDPB underlines that the purpose limitation principle contributes to transparency, legal certainty and predictability and aims to protect the

[304] See Section 5.1 on page 131 on this obligation.
[305] [De Hert and Gutwirth, 2006b].

data subject by setting limits on how controllers are able to use their data and reinforce the fairness of the processing.[306] Legal scholars connect concepts that vary from integrity, dignity, equality, autonomy or informational self-determination, to supporting democracy, the balance between and division of powers, fair trial, government transparency, pluralism, tradition and reducing the risk of harm.[307] In the following two Sections the concept of self-determination and the Rule of Law in relation to the purpose limitation principle will be discussed.[308]

3.4.1 Control, self-determination and autonomy

Various scholars, including Clarke, Colonna, Tzanou, Zarsky and Grafenstein place purpose limitation in light of the notion of control and the concepts of self-determination and autonomy.[309] Jasserand points out that the connection between purpose limitation on the one hand and control and the concept of self-determination on the other

[306] Article 29 Working Party *Opinion on Purpose Limitation*, 2013, WP 203, p. 11. Transparency, legal certainty and predictability are also underlined by the EU legislature in the field of criminal law enforcement, specifically in the area of law enforcement cooperation, where data subjects are usually unaware when their personal data are being collected and processed and where the use of personal data may have a very significant impact on the lives and freedoms of individuals. Recital 26 Europol Regulation; The EDPB also believes that compliance with the purpose limitation principle is essential to ensure fair and effective competition between economic players on the relevant markets. "Upholding the purpose limitation principle is essential to ensure that companies which have built monopolies or dominant positions before the development of big data technologies hold no undue advantage over newcomers to these markets." Article 29 Working Party *Statement on Statement of the WP29 on the impact of the development of big data on the protection of individuals with regard to the processing of their personal data in the EU*, 2014, WP 221, p. 2-3.

[307] [Gutwirth and de Hert, 2009, p. 5]; [Westin, 2003]; [Coudert et al., 2012]; [Brouwer, 2011, p. 276 and 239]; [Schermer, 2011, p. 47]; [Brouwer, 2008]; Blaustein connected privacy to the concept of dignity in the era of the first large scale databases. [Blaustein, 1964]; Zarsky refers to the EU tradition and the constitutional mandate in the CFREU that, in his eyes, legitimize the upholding of the purpose limitation principle for Europeans.[Zarsky, 2016, p. 1006]; See Roessler for an interdisciplinary view on privacy and data protection. [Roessler, 2015]; The EDPB and early working groups on data protection also theorized the purpose limitation principle. See for example: Article 29 Working Party *Statement on Statement of the WP29 on the impact of the development of big data on the protection of individuals with regard to the processing of their personal data in the EU*, 2014, WP 221, p. 2-3; Committee of Ministers of the Council of Europe Resolution on the Protection of the Privacy of Individuals vis-a-vis Electronic Data Banks in the Public Sector, (74) 29, par. 4.

[308] The author is well-aware that this is not an exhaustive list and other concepts have been brought in connection with the purpose limitation principle too.

[309] [Clarke, 1991]; [Colonna, 2014, p. 300-302]; [Tzanou, 2017, p. 40]; [Zarsky, 2013, p. 1541-1541]; [von Grafenstein, 2018, p. 102].

hand gets lost when personal data is processed for criminal law enforcement or public security purposes.[310] This is only partly true. Purpose limitation in private-to-public data transfers supports self-determination and enables control for the data subject in the choice of a data controller that will process her personal data. With the help of the purpose specification the data subject can pick a data controller that processes for criminal law enforcement purposes and voluntarily hand-over this data to competent authorities or she can pick a data controller that only hands-over her personal data to the competent authorities when there is a legal obligation to do so.[311]

The Explanatory Notes of the OECD Guidelines give a good illustration of the role of the purpose limitation principle in a data-driven society in connection with self-determination and autonomy. The Notes underline that data concerning opinions and evaluating data may easily be misleading if it is used for purposes to which it bears no relation.[312] The OECD recommends that at the moment personal data no longer serve a purpose the data should be deleted or made anonymous.[313]

The purpose limitation principle facilitates the demand that decisions about data subjects are motivated because the proportionality and subsidiarity of the data processing should be assessed in light of the processing purposes. Motivated decision making restricts processes that are solely based on big data and automated decision making. To this extent the principle protects against de-individualization: individuals will not be judged on the basis of group characteristics but on their character traits and attributes.[314] Purpose limitation therefore serves as a vindication of boundaries protecting each person's right not to be simplified, objectified, and evaluated out of context,[315] and protects life choices against any form of public control or social stigma.[316] The principle tempers the *datafication* of society and its negative effects to the rights and freedoms of the data subjects.[317]

[310] [Jasserand, 2018, p. 155].

[311] This topic is discussed in Section 5.4.3 on page 179.

[312] Explanatory Notes 2013 OECD Guidelines Governing The Protection Of Privacy And Transborder Flows Of Personal Data, par. 53; See also footnote [62].

[313] Explanatory Notes 2013 OECD Guidelines Governing The Protection Of Privacy And Transborder Flows Of Personal Data, par. 54.

[314] [Schermer, 2011, p. 47].

[315] [Rosen, 2000, p. 20].

[316] [Friedman, 1990, p. 184].

[317] [Hildebrandt, 2015b].

3.4.2 Purpose limitation and the Rule of Law

Hildebrandt stresses that purpose limitation is closely related to the central notion of the Rule of Law and that of the legality principle.[318] The Rule of Law is perhaps the most powerful and often repeated political ideal in contemporary[319] legal discourse.[320] It refers to the situation in which a ruler only gets power when she accepts the system of checks and balances that supports the exercise of power in a

[318] [Hildebrandt, 2014].

[319] The concept dates back to Aristotle. *The Politics of Aristotle*, book III, ch xi, 19 at 127; See for another older and somewhat bombastic description of the Rule of Law the pamphlet of Thomas Paine who tried to inspire colonialists on the American continent to fight for independence from Great Britain in the summer of 1776. [Paine, 2004]; See also [Scalia, 1989, p. 1176].

[320] The Rule of Law is known under partially concurrent expressions such as *legality*, *estado de derecho*, *état de droit*, *stato di diritto* and *Rechtsstaat*. [Craig, 1997, p. 12]; [Tamanaha, 2012, p. 1]; The implications of the linguistic variety can be illustrated by a case that was ruled by the CJEU in 1979. CJEU 13 February 1979, C-101/78, (*Granaria BV/Hoofdproduktschap voor Akkerbouwprodukten*) par. 5. The English version of the CJEU rulling speaks of the *Rule of Law*. In the German version the word *Rechtstaatlichkeid* is used. In German legal philosophy this concept is used to point to concrete manifestations of the *Rechtsstaat* idea, while *Rechtsstaatprinzip* is historically used to pinpoint the legal principle of constitutional value and is similar to the Rule of Law in English legal doctrine. For a comprehensive analysis of the usage and substance of these terms see: [Tiedeman, 2014] in English and [Kunig, 1986, p. 4-25] in German. The Dutch translators for this case law at the CJEU went for *wettigheidsbeginsel*: a strictly formal concept of legality in Belgian law doctrine. The French version speaks of *principe legalité*. This principle is often used in a more modest meaning that only covers the formal aspects of the Rule of Law. The notion of the *État de Droit* approximates the German substantive conception of the Rechtsstaat and similar more substantive conceptions of the Rule of Law in the context of Anglo-American law. [Hildebrandt, 2015a, p. 47]. In France the binding of the government to the Law was presumed to be an inherent aspect of a republic and is therefore only scarcely articulated in French legal literature. [Letourneur and Drago, 1958, p. 148] and [Pech, 2009, p. 37]. From these examples, it is apparent that all of these expressions have long-running definitional and normative disputations in national jurisprudence and in that capacity not always translate to the Rule of Law one-on-one. See for a broader analysis of the issues that emerge from the multilingual approach of the European institutions: [Ammon, 2006]. On the linguistic aspects of the concept of the Rule of Law in the global discourse, see [Sharandin and Kravchenko, 2014]. It would be incorrect to state that due to these differences there are no common denominators in the concept they try to encapsulate, and that therefore the Rule of Law fails as a widely acknowledged concept of law. Differently: [Loughlin, 2010, Chapter 11].

non-arbitrary manner.[321] The European Commission for Democracy through Law[322] described the Rule of Law as requiring everyone to be treated by all decision-makers with dignity, equality and rationality and in accordance with the law, and to have the opportunity to challenge decisions before independent and impartial courts for their unlawfulness, where they are accorded fair procedures.[323] This means that the exercise of authority should be reasonable, for the purpose for which the powers were conferred and without misuse by exceeding the limits of such powers.[324]

The purpose limitation principle has similar characteristics as described above. The data controller can only process data in a system of checks and balances and in a non-arbitrary manner by formulating the purpose prior to the collection of data and refrain from processing the data for purposes that are incompatible with the pre-determined conditions. The requirement that the processing purposes have to be legitimate, specific and explicit aids to treatment of the data subject with dignity, equality and rationality and in accordance with the law, and to facilitate to effective accountability claims, giving the data subject a stick to help challenge decisions of the data controller before a court for their unlawfulness.

The French enlightenment philosopher Montesquieu proposed a *relational notion of law* that aims to balance potential power relationships, by imposing checks and balances.[325] His *trias politica* theory was designed to serve this concept of law with the

[321] Report on the rule of law - Adopted by the Venice Commission at its 86th plenary session (Venice, 25-26 March 2011)[p. 5.]; see also [Rosenfeld, 2001, p. 4-5] on the effects of the negative formulations of the definition of the Rule of Law; The Rule of Law achieves the supremacy of law over arbitrary power, which is contrary to the Rule of Individuals. The Rule of Law in contrast to the Rule of Men is more popular because the concept of the Rule of Law was phrased in a period that still excluded women from the political domain. I agree with Margaret Radin that when considering the Rule of Law in modern times it should be distinguished from the Rule of Individuals. [Radin, 1989, p. 781]; In a society that escaped a despotic status, law should demand law and institutions, and no (legal) person is considered to be above the law, including the government and its representatives. Arbitrary decisions by government, government officials and private entities should not form the basis for legal detriments and their execution. [Chesterman, 2008, p. 4]; [Angelis and Harrison, 2003, p. 2].

[322] This commission is better known as the Venice Commission. It is the Council of Europe's advisory body on constitutional matters that provides legal advice to its member states and helps to ensure the dissemination and consolidation of a common European constitutional heritage.

[323] Report on the rule of law - Adopted by the Venice Commission at its 86th plenary session (Venice, 25-26 March 2011)[p. 5.]

[324] [Bingham, 2007, p. 78]; [O'Donnell, 2004, p. 33].

[325] [De Montesquieu, 1989]; [de Secondat et al., 2001]; The legality principle is a moral principle that underlines citizenship as a core value in law. [Foqué and Hart, 1990, p. 80].

separation of political power among a legislative-, executive-, and judiciary branch. Montesquieu argued that a system of power separation institutionalizes the mediation of power.[326] Through the separation of data operations, the mediation of power of the data controller can be institutionalized too.[327] The German Constitutional Court stressed the importance of division of informational powers in the 1980s, by explaining that the government does not consist of one 'informational unit', it is built up from different branches that need different information regimes in order to restrain its power.[328] Information asymmetries influence the level playing field between government and citizens, and between businesses and consumers.[329] The purpose limitation principle lays down the requirements for data processing to be compartmentalized into processing operations with a beginning, the specification of the purposes prior to the data collection, and an end, the fulfillment of the purposes. By putting limits on data processing, knowledge collection, exploitation and production is limited and the information symmetry and power balance safeguarded.[330]

[326] Interesting to note here is that Montesquieu published his masterpiece on the separation of powers anonymously in first instance. See [Rahe et al., 2001, p. 269]. The Rule of Law was considered a radical idea by the authorities. Nowadays some legal scholars refer to the threats to the Rule of Law, when arguing in favor of backdoors in cryptography for intelligence and law enforcement purposes, perhaps underestimating the function of cryptography for publishing anonymously. The separation of powers was once a radical idea and perhaps would still be if it wasn't for an anonymous publication method at the disposal of Montesquieu.

[327] [De Hert and Gutwirth, 2006a, p. 28]; Brouwer connects the purpose limitation principle to the notion of *good governance*, which is related to the separation of powers. She argues that the principles of good governance protects both the interests of the data subject and the data controller by guaranteeing the integrity, accuracy and duration of retention of the data. [Brouwer, 2011, p. 279]; See [Cleiren et al., 1990], who described the relationship between good administration and good governance in criminal law enforcement. In 1974 data processing was seen as a means of new administrative techniques which public authorities were using in order to assure the optimal performance of the tasks entrusted to them. The governance view on data processing is, therefore, nothing new. Preambule Committee of Ministers of the Council of Europe Resolution on the Protection of the Privacy of Individuals vis-a-vis Electronic Data Banks in the Public Sector, (74) 29.

[328] BVerfgE 65, 1, par. 46 and 69; De Hert and Gutwirth stated: "It would be disrespectful of the ideas behind data protection to see government as a whole that may use "its' information taken at random for whatever governmental database, let alone from private databases".[De Hert and Gutwirth, 2006a, p. 28].

[329] [Schermer, 2011, p. 47].

[330] Montesquieu theorized the role of citizens and concluded that a social order has more than one architect because it is determined by the type of power exercise, as well as by empirical, geographical and ecological circumstances. He introduced empirical research in social sciences by extending comparative methods of classification to the political forms and using the same research methods for the study of social

Governmental re-use of legal measures for new purposes, challenges the protective character of the law and can easily lead to misuse of power. It is at odds with the idea of *certainty of procedure*, which is considered a core aspect of the Rule of Law by a broad range of scholars.[331] In the context of data protection similar *certainty of procedure* problems can be seen, to which I refer as *mission creep*: the change in the interpretation of the explicit purpose specification which leads to further processing for new purposes without the proper communication of these new purposes.[332] The initial purpose specification is appropriated for the processing for new purposes. In cases of *mission creep* the purposes change but the data controller keeps referring to the same explicit purpose specification.[333] Mission creep is a type of *function creep*.[334] Other forms of *function creep* are *techno creep*: the further use of data processing in-

structure as were used in exact sciences. The object of his study was the relationship between power, political will and individuals. His study sharpened his views on how to channel power that lead to his view on the separation of power in his 1749 magnum opus *De l'esprit des lois*. The use of empirical data with focus on the relationship between actors in power – including the individual – changed the meaning of social studies and ultimately the way humans perceive humanity. Big data changes the method of research and with that the meaning of knowledge. Big data has the potential to give insight in the relationships of power. It could very well be that the outcome of big data analysis demands new theories and guiding principles on how to control power, just like the outcome of empirical research in social sciences led to the trias politica.

[331] Kotter argues that these scholars are equally distributed over the spectrum of cultural, political, and economic preferences. For this reason it is safe to say that certainty of procedure is a core aspect. [Mathias Kötter, 2014, p. 72] in [James R. Silkenat, 2014]; I agree, because even thin notions of the Rule of Law, like the those defended by Craig or Raz, underline the importance of certainty of procedure by limiting the purpose of conferred powers. Craig argues, for example, that in order to speak of the Rule of Law the legal framework must have certain specific procedural characteristics that address the way the law is promulgated, the clarity of the underlying norm, and the temporal dimension of the enacted norm. [Craig, 1997]. He states that "a government must be able to point to some basis for its action that is regarded as valid by the relevant legal system". [Craig, 2007]. Raz emphasizes the stability of law and interpretation by describing the Rule of Law as a state in which legal norms are prospective, adequately published and clear. Once enacted law should be relatively stable and law making should be open, stable, clear and based on general rules. The courts should be easily accessible and the discretion of crime preventing agencies should not be allowed to pervert the law. [Raz, 1977]; See also: [O'Donnell, 2004, p. 35].

[332] See in this context: [WODC, 2011].

[333] For example, the GCHQ, the British signals intelligence service, interpreted the word *collection* as some sort of querying the data that was gathered. See to this extent https://www.wired.co.uk/article/gchq-tempora-101. Lastly retrieved 22 December 2019; and ECtHR 13 September 2018, nos. 58170/13, 62322/14 and 24960/15 (*Big Brother Watch and others/the United Kingdom*).

[334] See [Clarke, 1991] on the topic of function creep.

frastructure for different purposes,[335] and *data creep*: the further use of personal data for different purposes than the ones for which the data is originally collected without reference to the initial purpose specification. All three types of function creep are considered a risk for data subjects as it may result in unanticipated use of personal data by the controller or by third parties. According to the EDPB purpose limitation safeguards against mission creep: the gradual widening or blurring of purposes for which data is processed after a data subject has agreed to the initial collection of the data.[336] The purpose specification requirement fulfills this function for all processing grounds not only when data is being processed on the base of consent.[337] What is more, next to protecting against mission creep[338] the purpose limitation principle also safeguards against data creep and techno creep. Data creep is at the core of the non-incompatibility requirement and the possibilities for techno creep are limited by the obligation to implement data protection by design and by default. This obligation stimulates the designers of systems to make decisions based on the processing purpose, which might lead to an increase in minimal purpose technology that minimizes the risk for techno creep.[339]

[335] Curry described this as the situation in which "a system developed for a particular purpose comes to be used for, or to provide the underpinning for other systems that are used for, different purposes". [Curry et al., 2004, p. 362]. A driving force behind mission creep is interoperability: the wish for interconnectivity. Interoperability means much more than just hooking op systems, but in EU policy this interoperability is framed as a purely technical matter in EU policy. [Bigo et al., 2012, p. 21]. Interoperability has a technical, semantic, social cultural, political, economic, organizational and legal dimension. [De Hert and Gutwirth, 2006a, p. 23].

[336] Article 29 Working Party *Guidelines on consent under Regulation 2016/679*, 2018. WP 259, p. 11-12. The EDPB speaks of function creep because it does not make the threefold distinction (data-, techno- and mission creep) in its opinions.

[337] See Section 4.1.2 of this study.

[338] Mission creep is also limited by certainty of procedure, because in many cases the purposes have to be codified in law, and the possibility of further use for compatible and incompatible purposes are laid down by law. See Section 4.2 on page 117 for the conditional function of the purpose specification requirement on human rights protection and the requirement of *in accordance with the law*.

[339] See Section 4.1.5.1 on page 112 of this study.

3.5 Position of purpose limitation in the data protection framework

This section describes the general position of the purpose limitation principle within the EU data protection framework. In general, processing of personal data has to meet four comprehensive touchstones in order to be legitimate under EU data protection law.[340] Firstly, the data processing has to meet the data protection principles – which include the purpose limitation principle – secondly, the processing should be based on at least one lawful processing ground,[341] thirdly, the controller should meet the data controller obligations, and, lastly, the data subjects should be able to effectively exercise their data subject rights. These touchstones are cumulative.[342] The most important effect of cumulation on the purpose limitation principle is that a (new) lawful processing ground cannot dismiss the data controller from her obligation to process the data in-line with the pre-determined conditions that were set at the moment of the data collection.[343]

The data controller is responsible for compliance with the data protection touchstones. For the purpose limitation principle, this includes a duty towards the data subject to avoid processing by third parties for incompatible purposes.[344] The scope

[340] This study includes accountability under the data protection principles. Some scholars point to accountability of the data controller as a fifth touchstone. This group includes the European Data Protection Supervisor Buttarelli, who explained that "Accountability should promote sustainable data processing, by ensuring that the burden of assessing the legality and fairness of complex processing falls primarily on controllers and regulators, not on the individual."[Buttarelli, 2016]; The update of the OECD guidelines in 2013 also indicate this fifth touchstone: the data protection principles remained unchanged. The changes focussed on more possibilities for redress for the data subject and the underlining of the accountability of the data controller.

[341] In the case law the data protection principles and legitimate processing grounds are often listed together. CJEU 20 May 2003, joined cases C-465/00, C-138/01, C-139/01, (*Rechnungshof/Österreichischer Rundfunk and Others, and Christa Neukomm and Joseph Lauermann/Österreichischer Rundfunk*), par. 65; CJEU 30 May 2013, C-342/12, (*Worten*), par. 33; CJEU 24 November 2011, C-468/10 and C-469/10, (*ASNEF and FECEMD*), par. 26; CJEU 13 May 2014, C-131/12, (*Google Spain SL, Google Inc./AEPD, Mario Costeja González*), par. 69.

[342] See section 5.1 of this study op page 131 for a discussion of the relationship between the requirement of non-incompatibility and the processing grounds.

[343] In Section 5.2 and 5.3 the derogations from this rule are described.

[344] Article 29 Working Party *Opinion 02/2012 on facial recognition in online and mobile services*, 2012, WP 192, p. 8: "Data controllers must ensure that digital images and templates are only used for the specified purpose for which they have been provided. Data controllers should put technical controls in place in order

of this obligation is not determined by the availability of the data; the mere fact that personal data is publicly available for a specific purpose does not mean that that personal data is open for re-use for any other purpose.[345] In an online environment where personal data is easily accessible this can be a challenge.

The concept of controller is a functional concept, intended to allocate responsibilities where the factual influence is, and thus based on a factual rather than a formal analysis; the entity that determines the processing purposes and means must be considered the data controller.[346] The "determination of purpose of processing" and "substantial questions that are essential to the core of the data processing" are reserved for the controller.[347] Where the purposes and means are determined by law, the controller or the specific criteria for its nomination can also be provided for by law.[348] The definition of *controller* is broad in order to achieve effective and complete protection of the rights and freedoms of data subjects.[349] The protection of rights as well as the responsibility and liability of controllers and processors, also in relation to the monitoring by and measures of supervisory authorities, requires a clear attribution of the responsibilities, including where a controller determines the purposes and means of the processing jointly with other controllers[350] or where a processing operation is carried out on behalf of a controller.[351]

Data controllers have the flexibility to delegate the data processing to another entity: a data processor.[352] This entity is bound to the data protection principles in

---

to reduce the risk that digital images are further processed by third parties for purposes for which the user has not consented to".

[345] Article 29 Working Party *Opinion 06/2013 on open data and public sector information ('PSI') reuse*, 2013, WP 207, p. 20.

[346] Article 29 Working Party *Opinion 1/2010 on the concepts of "controller" and "processor"*, 2010, WP 169, p. 9; Article 4(7) GDPR: The controller means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the data processing; ; See CJEU 20 May 2003, joined cases C-465/00, C-138/01, C-139/01 (*Rechnungshof/Österreichischer Rundfunk and Others, and Christa Neukomm and Joseph Lauermann/Österreichischer Rundfunk*) par. 64; CJEU 6 November 2003, C-101/01(*Bodil Lindqvist*) par. 24; CJEU16 December 2008, C-524/06, (*Huber/Germany*) par. 43.

[347] Article 29 Working Party *Opinion 1/2010 on the concepts of "controller" and "processor"*, 2010, WP 169, p. 15.

[348] Article 4(7) GDPR.

[349] CJEU 13 May 2014, C-131/12, (*Google Spain SL, Google Inc./AEPD, Mario Costeja González*), par 34.

[350] Article 26 GDPR; art. 21(1) LED.

[351] Article 28 GDPR; art. 22 LED juncto Recital 54 LED.

[352] The processor means a natural or legal person, public authority, agency or other body which processes

light of the instructions of the data controller.[353] The data processor's obligations towards the purpose limitation principle can be summarized to two rules: Firstly, the processor should only process the data for the legitimate purposes that are specified by the controller. Secondly, the processor cannot process the data for its own purposes nor for the purposes of a third party, even if those purposes appear to be compatible with the purposes as defined by the data controller.[354]

The following section details the cumulative data principles and lawful processing grounds. The data controller obligations and the data subjects rights are discussed in the next chapter where the conditionality of the purpose specification requirement on these touchstones is investigated.[355]

3.5.1 Purpose limitation as one of the data protection principles

The data protection principles are codified in binding international data protection law since 1981 with the signing of the Council of Europe Data Protection Convention.[356] In EU data protection law five principles can be distilled:

The principles of lawfulness and fairness These principles safeguard that personal data must be processed lawfully and fairly. The GDPR adds the principle of transparency.[357] The lawfulness principle relates to a broader sense of legitimacy than ticking off one of the lawful processing grounds. Just like the element of legitimate purposes, which was discussed in Section 3.3.2, lawfulness relates to the Rule of Law and the criterion of *in accordance with the law*. The fairness principle underlines the omnipresence of the demand of proportionality in data processing and the

personal data on behalf of the controller. See art. 4(8) GDPR.

[353] See Article 29 Working Party *Opinion 1/2010 on the concepts of "controller" and "processor"*, 2010, WP 169, p. 15.

[354] The processor can process the data for their own purposes when they become controllers of their own. See Article 29 Working Party *Opinion 1/2010 on the concepts of "controller" and "processor"*, 2010, WP 169; Article 29 Working Party *Recommendation 1/2012 on the Standard Application form for Approval of Binding Corporate Rules for the Transfer of Personal Data for Processing Activities*, 2012, WP 195a, p. 12.

[355] See in particular Section 4.1.4 on page 108 on the data subject rights and Section 4.1.5 on page 112 on the data controller obligations.

[356] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data no. 108.

[357] In this study that substance matter will be discussed in light of the data controller obligations and data subject rights.

transparency principle is further detailed in the data controller obligations that will be discussed in Section 4.1.5. These principles in relation to the purpose specification requirement are discussed in Section 4.1.3.1.

The purpose limitation principle The topic of this research is discussed throughout this study. This was already the case in Section 3.1 and Section 3.3. The purpose specification requirement is further researched in Chapter 4 and the non-incompatibility requirement in Chapter 5.

Data minimization This principle lays down that personal data must be adequate, relevant and limited to what is proportional in relation to the purposes for which they are processed. This principle is frequently read in conjunction with the purpose limitation principle and the storage limitation principle, and is discussed in Section 4.1.3.4 on page 106.

Accuracy The accuracy of the data principle lays down the obligation of the data controller to make sure personal data is accurate and, where necessary, kept up to date. The data controller must take every reasonable step to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay. This obligation is linked with the corresponding data protection rights of erasure and rectification for the data subject. Section 4.1.3.2 discusses the links between this principle and the purpose specification requirement.

Storage limitation Personal data must be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which they are processed. This rule is the core of the storage limitation principle. Some scholars have incorporated this rule in the purpose limitation principle. An example of this is the purpose limitation definition of Brouwer that was described on page 60.

Integrity and confidentiality This principle safeguards that personal data is processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures. The

new regulatory framework expanded the scope of the right and obligations that follow from this principle to the obligatory data breach notifications and explicit data security obligations. Section 4.1.5.3 discusses the relationship between the purpose specification requirement and these obligations.[358]

The data protection principles should be considered in light of each other and cannot be applied separately. The principles can, however, be grouped in different types in light of the fundamental right to protection of personal data ex art. 8 CFREU. This is discussed in Section 5.2.1.2 on page 154.

3.5.2 Cumulation with the lawful processing grounds

All data processing must be based on a lawful processing ground. In the field of criminal law enforcement and public security processing is only lawful when it is based on necessity and a law.[359] The GDPR provides so-called *necessity grounds* and the *consent ground*.[360] The necessity grounds include: a contract, a legal obligation,[361] vital interests, the performance of a task carried out in the public interest, and the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data.[362] Consent is only valid when it qualifies as a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing ex art. 4(11) juncto art. 7 GDPR.[363] Recital 43 GDPR explains that consent cannot provide a valid legal ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject and the controller, in particular where the controller is a public authority which makes it unlikely that consent was freely given in all the circumstances of that specific situa-

[358] See also Section 4.2.4 of this study.

[359] See Section 4.1.2.

[360] Please see Section 4.1.2.1 on page 97 for the discussion of consent and necessity. This lawful processing ground is also connected to the criterion of necessity, because consent should be given for one or more purposes and data can only be processed when it is necessary in relation to those purposes, pursuant to art. 5(1)(c) GDPR. See Section 4.1.2 and Section 4.1.3.4 on this matter in relation to the purpose specification requirement.

[361] This ground will be further discussed in Section 5.2.2 from page 156 onwards.

[362] This so-called *f-ground* is in detail discussed in Section 5.4.2.

[363] See also Recital 32, 42 and 43 GDPR. See also [Gutwirth et al., 2009, p. 2].

tion.[364] Consent covers all aspects of processing relating to the fulfillment of a purpose, including for example the passing of personal data to another undertaking of the data controller and processing for the same purpose but with different means.[365] The processing ground consent cannot be used for all processing operations.[366] In the *Schwarz*-case, for example, the CJEU explained that because it is essential for EU citizens to own a passport in order to, for example, travel to non-EU countries, EU citizens wishing to make such journeys are not free to object to the processing of their personal data in the process of issuing the passport. In those circumstances, persons applying for passports cannot be deemed to have consented to that processing, and the processing will have to be based on another legitimate processing ground.[367]

3.5.3 Safeguard in the protection of the rights and freedoms of the data subject in vertical relationships

Purpose limitation applies to horizontal relationships between data subjects and private entities, as well as to vertical relationships between data subjects and public authorities. The European legislature acknowledged the vulnerability of the latter type of relationship under the Rule of Law.[368] To that end, the legislature se-

[364] See in this regard also the Article 29 Working Party *Opinion on Consent*, 2011, WP 187; and Recital 35 LED.

[365] CJEU 15 May 2011, C-543/09, (*Deutsche Telekom AG/Germany*), par. 65.

[366] The GDPR conditions for consent are stated in article 7 GDPR: 1. Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data. 2. If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding. 3. The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent. 4. When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.

[367] CJEU 10 October 2013, C-291/12, (*Michael Schwarz/Stadt Bochum*), par. 32; See to this extent also the EDPB opinions on power balances and consent: Article 29 Working Party *Opinion on Consent*, 2011, WP 187, p. 12-14; Article 29 Working Party *Opinion 2/2017 on data processing at work*, 2017 WP 249.

[368] See Section 3.4.2 on page 74 on the relationship between the purpose limitation principle and the Rule of Law.

cured in art. 6(3) GDPR that the explicit purpose specification must be established in the legislative measures on which public authorities base their data processing at all times.[369] The European data protection framework permits the Union and national legislature to restrict some data protection principles, data subject rights and controller obligations ex art. 23 GDPR.[370] These restrictions embody the power imbalances between the data subject and government and are, therefore, accompanied by checks and balances, including the requirement that the restriction must be laid down in a legislative measure that contains the explicit purpose specification ex art. 23(2)(a) GDPR. This requirement also applies to derogations from the non-incompatibility requirement of the purpose limitation principle ex art. 6(4) juncto 6(1)(c) and art. 6(3) GDPR. [371] In accordance with the case law of the CJEU and ECtHR, these legislative measures do not necessarily have to be legislative acts adopted by a parliament, but they should be clear and precise, and their application should be foreseeable to persons subject to it.[372]

This protective function of purpose limitation in vertical relationships has its roots in the case law of the CJEU. It was underlined for the first time by the Advocate-General in the *Promusicae*-case, that dealt with the functioning and scope of the restriction clauses that preceded 6(4) juncto art. 23 and GDPR and art. 11b ePrivacy Regulation.[373] The case concerned the further processing of personal data for purposes that were incompatible with the initial purposes. Promusicae, a Spanish representative of collective rights holders for producers and publishers of music, brought an action against an internet service provider in order to obtain personal data of the provider's costumers with a view to bringing civil judicial proceedings against

[369] Article 6(1)(c) and (e) juncto art. 6(3) GDPR; art. 8(1) juncto art. 8(2) LED. This obligation applies to data processing for initial purposes and all further processing for new purposes.

[370] This will be discussed in Section 5.2.1.1 on page 153 in light of the further processing of personal data.

[371] The derogation clause for the non-incompatibility requirement is discussed in Section 5.2.2 on page 156.

[372] Recital 41 and 45 GDPR and Recital 33 LED.

[373] At that moment art. 13 DPD and art. 15 ePrivacy Directive; The ePrivacy Regulation is has not been adopted when lastly checked on 22 December 2019. The version used in this study is: Committee report tabled for plenary, 1st reading/single reading, Draft European Parliament Legislative Resolution on the proposal for a regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications, Amendment 121 amending art. 11b(new) ePrivacy Regulation).

the costumers. In the eyes of Promusicae these costumers allegedly illegally downloaded music of which members of Promusicae held the exploitation rights. At the moment of litigation the internet service provider was retaining costumer data under national legislation that implemented the Data Retention Directive.[374] That Directive obligated Member States to implement legislation that forced organizations, such as internet service providers, to temporarily further process some of the personal data, including telecommunications metadata, they hold on their costumers for the purpose of keeping this data available for the investigation and prosecution of serious crime.

The Advocate-General concluded that the purposes of the Data Retention Directive and Promusicae were incompatible and that neither the European- nor the national legislature had taken any decision on retention of personal data for the purpose of acting against copyright infringements by means of civil proceedings.[375] The Advocate-General stressed that it would not have been foreseeable to infer secondary processing purposes which were not expressly specified in restricting measures because this would be contrary to the requirement of foreseeability and the purpose limitation principle.[376] The CJEU confirmed the position of the Advocate-General,[377] and in later case law repeated that restricting measures on the data subject rights, data controller obligations or data protection principles require explicit purpose spec-

[374] This directive was later in a separate and unrelated case annulled by the CJEU. See CJEU 8 April 2014, joined cases C-293/12, C-594/12, (*Digital Rights Ireland Ltd/Ireland, and Kärntner Landesregierung/Michael Seitlinger, Christof Tschohl and others*).

[375] Opinion A-G, CJEU 18 July 2007, C-275/06, (*Productores de Música de España (Promusicae)/Telefónica de España SAU.*), par. 95-111.

[376] Opinion A-G, CJEU 18 July 2007, C-275/06, (*Productores de Música de España (Promusicae)/Telefónica de España SAU.*), par. 95-111.

[377] CJEU 29 January 2008, C-275/06, (*Productores de Música de España (Promusicae)/Telefónica de España SAU*), par. 49-55. The CJEU indirectly concluded that at that time the Spanish legislative framework did not foresee in restrictions on the rights, obligations and principles by laying down an obligation to further use personal data and communicate that to rights-holders for the purpose of ensuring effective protection of copyright in the context of civil proceedings.The CJEU underlined that the EU legal framework leaves room to the national legislature to make such restriction, but that these restrictions are not obligatory. The CJEU added that when implementing the measures transposing EU directives, the authorities and courts of the Member States must not only interpret their national law in a manner consistent with those directives but also make sure that they do not rely on an interpretation of them which would be in conflict with those fundamental rights or with the other general principles of Community law, such as the principle of proportionality. CJEU 29 January 2008, C-275/06, (*Productores de Música de España (Promusicae)/Telefónica de España SAU*), par. 70.

ification in a EU or national legislative measures.[378] This requirement is now codified in art. 23(2) GDPR.

3.6 Conclusion on the general notion of purpose limitation

When looking at the European data protection framework and the balance that frameworks seeks to secure between the protection of fundamental rights and freedoms of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data, the role of the purpose limitation principle is right in the centre of that framework. On the one hand the principle seeks to protect the fundamental rights of the data subject while on the other hands it encourages the free flow of personal data by facilitating the further processing for compatible purposes. This role is expressed in the following obligations for the data controller: The purpose limitation principle obligates the controller to define the purposes prior to the processing and binds the controller to those predetermined purposes.

The purpose specification requirement prohibits unspecified data collection. The specification of the purposes *ex ante* is the yardstick in the enforcement of the data protection framework *ex post*. The purposes of processing can be distilled by looking at the answer to the question: Why is this data being processed? This answer has to be precise enough to base further proportionality questions on. The processing purposes have to meet a substantive notion of legitimacy, that – when the data processing falls under the ambit of art. 8(1) ECHR and art. 7 CFREU – corresponds with a legitimate aim. A non-expert person must be able to understand what data processing is and what data processing is not included in the data processing operation. The purpose limitation principle forces the data controller, therefore, to reflect on the data processing.

The non-incompatibility requirement forces data processing to be limited to the

[378] CJEU 10 October 2013, C-291/12, (*Michael Schwarz/Stadt Bochum*); CJEU 16 April 2015, C-446/12, C-447/12, C-448/12, C-449/12, (*W. P. Willems/Burgemeester van Nuth, H. J. Kooistra/Burgemeester van Skarsterlân, M. Roest/Burgemeester van Amsterdam, L. J. A. van Luijk/Burgemeester van Den Haag*). Section 5.1.2.2.1 on page 139 critically discusses the interpretation of the CJEU with regard to the non-incompatibility requirement.

predetermined purposes of the data processing operation. The non-incompatibility requirement limits the use of the data on the basis of the compatibility of the new purposes compared to the purposes that were determined at the moment of the initial data processing.

The purpose limitation principle is brought into connection with the autonomy because it protects the data subject against being simplified, objectified and evaluated out of context. The principle is also connected to the Rule of Law, in particular the concepts of certainty of procedure through protection against various forms of function creep, as well as the devision of power, by introducing informational borders for administrative and enforcement powers. Within the EU legal framework the principle is used for the protection against power imbalances in vertical and horizontal relationships.

Under data protection law the purpose limitation principle is situated between the other data protection principles, which form one of the four touchstones of data processing. Touchstone one entails that the data protection principles must be protected; Two, that the processing must be based on a lawful processing ground; Three, that the data controller obligations must be fulfilled; and, Four, that the data subject rights must be guaranteed. These touchstones are cumulating in the sense that all four must fulfilled in order for the data processing operation to be legitimate under EU data protection law.

Chapter 4

The purpose specification requirement

This chapter investigates the role of the purpose specification requirement in data protection law and its role in fundamental rights law. Section 4.1 discusses the connection between the requirement and various other central concepts of secondary data protection law. Section 4.2 investigates the role of the requirement in the fundamental rights framework on the protection of privacy and personal data ex art. 8 ECHR and art. 7 and 8 CFREU.

4.1 The conditional function of the purpose specification requirement

This section investigate the answer to the subquestion: What is the role of the purpose specification requirement in data protection law? The purpose specification requirement has an autonomous function, in which it embodies an independent principle that serves the legitimacy of data processing, and a conditional function, in which the requirement connects to a plethora of other principles and rules in data protection- and fundamental rights law. The autonomous function of the purpose specification requirement is well-recognized, and relates to its function in the purpose limitation principle as a safeguard in the protection of the rights and freedoms of the data subject and the support of the Rule of Law. For a discussion of this function I refer to Sections 3.1, 3.3 and 3.5.[379]

The conditional function expanded over time, and with the coming into force of the LED and the GDPR, the purpose specification requirement became a prominent

[379] See also Section 2.2 which gave an overview of the codifications of the purpose limitation principle in European data protection law.

parameter in the application of other data protection principles, data subject rights and data controller obligations. In this section the dependencies of other data protection rules for their their applicability, application or outcome on the purpose specification requirement is discussed. This dependency can be directly on the requirement itself, but also indirectly, on the purpose specification or the processing purposes.[380]

4.1.1 The determination of roles

The purposes of processing determine the roles of the actors involved in the data processing, including the role of the data controller and data processor, the recipient of personal data, and the leading supervisory authority. These different roles direct legal accountability, the scope of obligations of the data controller and the scope of the rights of the data subject when data is disclosed to a third party under the LED, and the enforcement jurisdiction of the supervisory authority under the GDPR.

4.1.1.1 The role of data controller and accountability

Besides discussing the role of the purpose specification requirement in data protection law, this section will contribute in answering the subquestion: Are the criteria for determining accountability and qualifying the data controller and the data processor under the European data protection framework similar to the criteria of accountability under fundamental rights law where competent authorities collect data with the help of informants? This section discusses the criteria for determining accountability under data protection law.

The data controller is defined as the entity who alone or jointly with others determines the purposes and means of the data processing.[381] As discussed on page 80, the data controller is the actor with effective control over the processing purposes. The identification of the data controller is, therefore, dependent on the processing purposes. Decisions on the means of processing, specifically those on technical or organizational aspects, can be delegated by the controller to a data processor,[382] but

[380] See Section 1.3.1 on page 11 for the vocabulary that is used in this study.

[381] ex art. 4(7) GDPR or art. 3(8) LED. Sometimes the data controller is apointed in the legislative measure that foresees in the data processing.

[382] See Section 3.5 on page 80 on the relationship between the data controller and data processor.

decisions on the processing purposes cannot be delegated.[383] If the data processor oversteps the agreement with the data controller, and starts processing the personal data for new purposes without being instructed to do so by the data controller, the data processor becomes the data controller of the processing operation for these new purposes.[384] The actor that qualifies as the data controller is accountable for the data processing,[385] bears the responsibility for the implementation of appropriate technical and organizational measures, and should be able to demonstrate compliance with the data protection principles, including the effectiveness of the measures.[386] The data controller cannot determine her liability by way of incorrect purpose specification, because as explained on page 80, European data protection law allocates the responsibilities to where the factual influence is.

The processing purposes condition the accountability of the different actors involved in the data processing. In case the purpose limitation principle would be replaced by the a system such as legitimate processing based on the interest of the data controller as proposed by Moerel and Prins and discussed on page 5 of this study, the attribution of accountability to the different actors would face serious problems. Competent authorities can have far more interest in the data processing of private entities than the entities themselves. When an expensive predictive policing pilot in a country is dependent on commercial data from a specific data broker because of the unique interoperability of the databases of the private entity with the databases of the competent authority, the interest of the competent authority in the continuation of the data processing by the private entity with the interoperable means is far greater than the interests to do so of the private entity. In this example, the purposes of data processing are still determined by the private entity: as a business model data is collected and sold to criminal law enforcement authorities. The private entity determines what type of data is collected, what type of inferences are made, what type of law enforcement agencies can subscribe to the service, what type of interoperability connections are used, and the terms of usage. The interest of the data controller will point to accountability for the criminal law enforcement authority, while the true

[383] Article 29 Working Party *Opinion 1/2010 on the concepts of "controller" and "processor"*, 2010, WP 169, p. 15.

[384] Article 28(10) GDPR; art. 22(5) LED.

[385] Article 5(2) GDPR and art. 4(4) LED.

[386] Recital 74, art. 5(1) juncto 24 GDPR; recital 50, 53, art. 4(4) juncto 19 LED. See [Raab, 2016] for a exploration of the dimension of the concept of accountability in the GDPR.

control lies with the data broker.

4.1.1.2 The role of recipient and receiver and its effect on data controller obligations and data subject rights

Under certain circumstances, a data controller can transfer personal data to another data controller. In general the European data protection framework refers to data controllers to whom data is disclosed as *recipients* ex art. 3(9) GDPR and art. 3(10) LED. The European data protection framework specifies a subset of data controllers that do not meet the qualification of recipient: public authorities which receive personal data in the framework of a particular inquiry in accordance with Member State law.[387] The legislature, however, did not define a concept for this subset. Because this distinction is important for this study, I introduce the term *receiver*[388] for a public authority to whom the data is disclosed in the framework of a particular inquiry in accordance with Member State law.[389] The qualification recipient/receiver influences the data controller obligations of the transferring data controller, and the data subject rights of the persons to whom the data relates.

Pursuant to art. 3(10) LED receivers are defined as public authorities to which personal data are disclosed in accordance with a legal obligation for the exercise of their official mission when they receive data that is necessary to carry out a particular inquiry in the general interest in accordance with Union or Member State law. The GDPR puts forward a different definition in art. 4(9): public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of that data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing. These public authorities are, for example, tax and customs authorities, financial investigation units, independent administrative authorities, or financial market authorities responsible for the regulation and supervision of securities markets.[390] The processing purposes of the public authority to whom the data is disclosed will reveal if the personal data will be processed

[387] Depending on the applicable legal framework this definition can be more extensive. See the next paragraph to this extent.

[388] This is my own terminology. I am not aware of a settled term to refer to this role in data protection doctrine or law.

[389] See previous footnote.

[390] Recital 22 LED and Recital 31 GDPR.

for a particular inquiry in accordance with a legal obligation for the exercise of their official mission or not. The qualification recipient/receiver is, therefore, directed by the processing purposes and when the processing purposes are specified in the law that provides the competence for the competent authority, the purpose specification directs the qualification.

The LED forces Member States to adopt legislation that obligates a transferring data controller to inform a recipient of specific conditions for processing and the requirement to comply with them.[391] No obligation exists for the Member States to adopt legislation of this kind for disclosures to a receiver. The transferring data controller is obligated to notify recipients of personal data of requests for rectification, erasure or restriction by the data subject.[392] There is no such obligation for the transferring controller after she disclosed personal data to receivers. Similarly, there is no obligation for the transferring data controller to notify a receiver to whom incorrect personal data have been disclosed or to whom personal data have been unlawfully disclosed. This obligation does exist for disclosures to recipients under the LED.[393]

Transparency of processing supports the effective exercise of data subject rights and enforcement by supervisory authorities. The transparency requirements of the LED towards disclosures to recipients are different to those towards disclosures to receivers. The data processing is more opaque when data is disclosed to receivers. For example, when data is transferred to a receiver there is no obligation for the transferring controller to maintain a record or log of the data disclosure.[394] What is more, the data controller does not have to inform the data subject about the categories of receivers to whom data is disclosed.[395] A specific access request of the data subject makes no difference to this.[396]

Because the processing purposes of the receiving public authority determine its role as recipient or receiver of personal data, the purpose specification requirement is connected to the scope of the data controller obligations and data subject rights. The question is if, and if so, in what circumstances, the receiving competent authority in

[391] Article 9(3) LED.
[392] Article 16(1), (2), (3) and (6) LED; art. 19 GDPR.
[393] Article 7(3) LED.
[394] Article 24(c) and 25(1) LED; art. 30 GDPR.
[395] This obligation only exists for categories of recipients. Article 13(2)(c) LED and Recital 43 LED; art. 13(1)(e) and 14(1)(e) GDPR and Recital 61 GDPR.
[396] Article 14(c) and 15 LED; and art. 15(1)(c) GDPR and Recital 63 GDPR.

public-private partnerships for the detection of crime should be considered a receiver. Recital 31 GDPR explains that public authorities to which personal data are disclosed in accordance with a legal obligation for the exercise of their official mission should not be regarded as recipients if they receive personal data which are necessary to carry out a particular inquiry in the general interest, in accordance with Union or Member State law. Also, the requests for disclosure sent by the public authorities should always be in writing, reasoned, occasional and should not concern the entirety of a filing system or lead to the interconnection of filing systems. The processing of personal data by those public authorities should comply with the applicable data-protection rules according to the purposes of the processing. The GDPR does not include criminal law enforcement authorities as an example of receivers, and the examples that are presented, are all in the domain of administrative law enforcement.[397] On the other hand, competent authorities are public authorities to which personal data can be disclosed in accordance with a legal obligation for the exercise of their official mission carrying out a particular inquiry in the general interest, in accordance with Union or Member State law.

In my opinion mandatory disclosure of personal data that is held by a private entity to a competent authority for the detection of crime in a specific inquiry qualifies as disclosure to a receiver, that should be based on a *lex specialis* as required in art. 6(4) GDPR.[398] These transfers are more opaque. For voluntary disclosures, one of the rationale of this study, no legal obligation is underlying the transfer, and the competent authority to whom the data is disclosed cannot qualify as a receiver and should instead be considered a recipient of the personal data. For these transfers the GDPR demands transparency. In Section 5.4.2 the legal regime for voluntary data transfers from private entities under the GDPR to competent authorities under the LED is further researched.

[397] Recital 31 GDPR.

[398] Restrictions of other rights and obligations, such as restrictions on the obligation to notify the data subject of the disclosure may be added pursuant to the art. 23(1) GDPR restriction clause; There is another subset of mandatory disclosures that do not follow a warrant but are initiated by the disclosing party due to a legal obligation to report certain types of crime. See for example art. 160 and 162 of the Dutch Criminal Enforcement Code (Wetboek van Strafvordering).

4.1.1.3 The role of lead supervisory authority in cross-border processing operations

The supervisory authority that can lead the enforcement of the GDPR in cross-border data processing operations is vested in the same jurisdiction as the main establishment of the data controller.[399] According to the CJEU case law, the concept of *establishment* has a flexible definition that departs from a formal approach that only checks the database of the Chamber of Commerce.[400] An establishment is defined by the specific nature of the economic activities and provision of services concerned, and involves the actual pursuit of economic activity through a fixed and stable arrangement for an indefinite or given period.[401]

When this assessment leads to the identification of establishments in more than one Member State, the purposes of processing are a determinant in the consideration for the main establishment. The main establishment is the place of the central administration of the controller in the Union, unless there is another establishment in the Union that takes decisions on the purposes and means of the processing of personal data, and has the power to have such decisions implemented.[402] In that case, the latter establishment is considered the main establishment. The purpose specification and the processing purposes condition the identification of the main establishment, and consequently the appointment of the lead supervisory authority for cross-border processing operation.

[399] Article 56(1) GDPR; The lead supervisory authority is the sole interlocutor of the controller or processor for the cross-border processing carried out by that controller or processor ex art. 56(6) GDPR.

[400] CJEU 1 October 2015, C-230/14, (*Weltimmo*), par. 29.

[401] Recital 22 GDPR; The concept *establishment* has its roots outside data protection law in EU consumer and tax law; CJEU 7 July 1985, C-168/84 (*Gunter Berkholz/Finanzamt Hamburg-Mitte-Altstadt*)par. 19; CJEU 25 July 1991, C-221/89 (*The Queen/Secretary of State for Transport, ex parte Factortame Ltd and others*) par. 20; CJEU 7 May 1998, C-390/96 (*Lease Plan Luxembourg SA/Belgische Staat*), par. 26; Recital 19 e-Commerce Directive; Article 29 Working Party *Working document on determining the international application of EU data protection law to personal data processing on the internet by non-EU based websites*, 2002, WP 56, p. 8; The stable arrangements can be determined by e.g. the appointment of a representative for costumer and legal disputes, a bank account in the EU and or a postbox. CJEU 1 October 2015, C-230/14, (*Weltimmo*), par. 33.

[402] When no single establishment has this task, the main establishment is the place of the controller's central administration in the Union. Article 4(16) GDPR. See in this regard also CJEU 13 May 2014, C-131/12, (*Google Spain SL, Google Inc./AEPD, Mario Costeja González*), par. 55-57.

4.1.2 The lawfulness of the processing

The purpose specification requirement is conditional for the lawfulness of the processing of personal data under the GDPR and the LED. Data processing that falls under the scope of the GDPR can be based on a *necessity ground* or on the *consent ground*.[403] Under the LED data processing is only lawful when it is necessary for the performance of the tasks of the competent authorities. The following Sections discuss the relationship between the purpose specification requirement and the lawful processing grounds.

4.1.2.1 Necessity as a processing ground

The processing grounds that are postulated in art. 6(1) sub (b) to (f) GDPR and art. 8(1) LED are directly based on *necessity*.[404]

The concept of *necessity* has its own independent meaning in Union law[405] and should be interpreted in a manner which fully reflects the objective of the legislation in which it is incorporated.[406] It has a long history in Union law and is well-established as part of the proportionality test.[407] When data processing is incompatible with the proportionality requirements that are derived from fundamental rights law, the data processing is also incapable of satisfying one of these requirements of proportionality and necessity in data protection law.[408] However, it does not mean that when the processing operation will not pass any of the necessity test in data protection law, the data processing inter alia violates fundamental rights. See to this extent also Section 4.2.3 on page 121. Under the GDPR, explicit and specific purposes are necessary to make the proportionality assessment prior to the application of the legitimate processing grounds ex art. 6(1) GDPR.[409]

[403] See page 83 of this study.

[404] See Section 2.1.2.4.3 on page 42 for a critique on the omission of this criterion in art. 8 CFREU. Article 5(1)(c) GDPR connects consent to the necessity criterion too. See for the connection of data minimization and the purpose limitation principle Section 4.1.3.4 on page 106.

[405] In Section 5.2.2.3.3 on page 167 proportionality and necessity in light of the Charter and the ECHR is discussed in the context of further use of personal data for incompatible processing purposes.

[406] CJEU 16 December 2008, C-524/06, (*Huber/Germany*), par. 52.

[407] See to this extent also Section 4.2.3 on page 121.

[408] CJEU 20 May 2003, joined cases C-465/00, C-138/01, C-139/01, (*Rechnungshof/Österreichischer Rundfunk and Others, and Christa Neukomm and Joseph Lauermann/Österreichischer Rundfunk*), par. 91.

[409] CJEU 16 December 2008, C-524/06, (*Huber/Germany*), par. 62; CJEU 30 May 2013, C-342/12,

The function of *necessity* is to delimit precisely the situations in which the processing of personal data is lawful and personal data should be processed only if the purpose of the processing could not reasonably be fulfilled by other means.[410] Necessity and proportionality are concepts that are used though-out the European data protection framework. The various tests that implement these concepts answer in my opinion three questions, of which necessity in relation to the legitimate processing grounds is the first that should be answered: *Is personal data the type of information that should be processed in order to pursue the processing purposes?* Once the decision is made on the first question, the second questions focusses on the subsidiarity of the processing of personal: *Is it necessary to process* this *personal data to pursue the processing purposes, or can the processing purposes be fulfilled with the use of different – less privacy-invasive – personal data?*[411] In my opinion this question is embedded in the proportionality test that has been laid down in the data minimization principle ex art. 5(1)(c) GDPR and art. 4(1)(c) LED. The third necessity question relates to the processing operation by the time the processing started. *Is the processing operation limited to the minimum necessary to fulfill the purposes of processing?* This type of proportionality is implemented in the storage limitation principle ex art. 5(1)(e) GDPR and art. 4(1)(e) LED.

The processing ground *consent* is enclosed in art. 6(1)(a) of the GDPR. The text of that provision does not directly refer to the necessity of the processing in terms of the first question that was discussed in the previous paragraph. However, because of the applicability of the data protection principles to all data processing operations under the GDPR, the second and third necessity question have to be answered irrespectively of the processing ground. To answer these latter questions the first question has to be answered too, because data processing can never meet the subsidiary and proportionality requirement when it was not necessary to process personal data to begin with.[412]

(*Worten*), par. 37 and 43; Article 18 Europol Regulation has a similar dependence of the necessity criterion on the processing purposes.

[410] CJEU 16 December 2008, C-524/06, (*Huber/Germany*), par. 52; Recital 26 LED.

[411] See to this extent for example the privacy enhancing technology attribute-based credentials. [Koning et al., 2014].

[412] See the next subsection for a discussion of art. 6(1)(a) GDPR in relation to the purpose limitation principle.

4.1.2.2 Consent for one or more specific purposes

Article 6(1)(a) GDPR prescribes that the consent of the data subject to the processing of her personal data is only lawful when it is given for one or more purposes. So, in order for consent to be legitimate, the purposes have to be specified and made explicit prior to the processing. Section 3.5.2 on page 83 of this study described that consent is defined as any freely given, specific, informed and unambiguous indication of the data subject's wishes and agreement to the data processing.[413] Recital 42 GDPR explains that for informed consent the data subject should be aware at least of the identity of the controller and the purposes of the processing for which the personal data are intended. An explicit purpose specification by the data controller enables the data subject to make a deliberate choice on trusting the data controller with her personal data as she will learn how and why her data will be processed, and will be able to rely on the limitative purpose description.[414] The lawful indication of the data subject's wishes and with that the lawfulness of processing that is based on consent is dependent on the processing purposes.

4.1.2.3 Further processing under the scope of the LED

Besides giving a better understanding into the role of the purpose specification requirement, this section contributes the answering of the subquestion: What is the relationship between the purpose specification requirement and other types of use limitation? Article 4(2) LED lays down the rules for incompatible further processing under the scope of the LED, which will be discussed in Section 5.5 in light of its use limitation aspects. Re-use of data is permitted under this provision when it meets the justification criteria stemming from fundamental rights: legitimate aim, proportionality and necessity, and legality.[415] This provision is formulated as a derogation to the non-incompatibility requirement.[416] On page 187 I argue that, based on the scope

[413] Article 4(11) GDPR. This definition applies to all occurrences of *consent* in the GDPR, including consenting on not fully identified purposes of scientific research. See footnote 293 on page 68 on this matter.

[414] Article 29 Working Party *Opinion 02/2013 on apps on smart devices*, 2013, WP 202, p. 17.

[415] These criteria are further elaborated on in the context of purpose specification in Section 4.2 and the context of further processing of personal data in Section 5.2.2.3.

[416] See Principle 5 R(87) 15. That recommendation was adopted to guide Member States in the restricting the data protection principles that are laid down in the DPC. See Section 2.2.1.2 and Section 2.2.1.1.

and positioning of art. 4(2) LED in the data protection framework, this provision shifts the default for data processing under the LED from use limitation based on the compatibility of the processing purposes to use limitation based on the justification criteria stemming from fundamental rights law. The application of art. 4(2) LED is dependent on the purposes of processing because it forces the data controller to execute a compatibility test before the provision itself can be invoked. As will be discussed in Section 4.1.3.3, it is impossible to execute a compatibility test without the purpose specification requirement. Once the provision can be invoked the purpose specification is necessary to, firstly verify if the new processing purposes pursue the criminal law enforcement and public security objectives that are listed in art. 1(1) LED, and, secondly, to check the authorizations for such data processing by the data controller and lastly to make a proportionality assessment. Sections 4.2 and 4.2 discuss the role of the purpose specification requirement in the justification of fundamental rights interferences.

4.1.2.4 Lawfulness of processing special categories of data

Special categories of data are by their nature particularly sensitive in relation to fundamental rights and freedoms and, therefore, merit specific protection.[417] The GDPR lays down a general prohibition on the processing of such data, from which derogation is only allowed when specific safeguards are in place and where the data subject gives her explicit consent ex art. 9(2)(a) GDPR or where one of the conditions of art. 9(2)(b)-(j) GDPR applies.[418]

Section 4.1.2.1 op page 97 discussed the connection between the lawful processing grounds, including consent and necessity, and the purpose specification requirement. A similar connection can be found between the rules for the derogations from

[417] These categories are processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation. Article 9(1) GDPR, art. 10 LED; Recital 51 GDPR.

[418] The Europol Regulation lays down a similar prohibition that can be lifted when the processing of special categories of data is strictly necessary and proportionate for preventing or combating crime that falls within Europol's objectives and if those data supplement other personal data processed by Europol. The selection of a particular group of persons solely on the basis of such personal data is prohibited. Article 30(2) Europol Regulation; The LED instructs Member States to lay down more stringent rules for such processing. See art. 10 LED.

the prohibition on the processing of special categories of personal data and the processing purposes. These derogations are dependent on the processing purposes for the lawfulness of *consent* ex art. 9(2)(a) GDPR, the necessity assessment that is embedded in the criterion of *necessity* ex art. 9(2)(c), (f), (g), (h), (i) and (j) GDPR, and to assess if personal data is indeed processed in a certain context ex art. 9(2)(b) and (d) GDPR. The purposes of processing are a determinant in the lifting of the ban on processing of special categories of personal data.

4.1.2.5 Lawfulness of data transfers without an adequacy decision or appropriate safeguards

Purpose specification is conditional for the lawfulness of international data transfers that are not based on an adequacy decision or appropriate safeguards. Under the GDPR data transfers to third countries or international organizations may in general take place only after the European Commission has taken an adequacy decision ex art. 45(1) GDPR or the transfer is accompanied by appropriate safeguards ex art. 46(1) GDPR. Article 49 GDPR, however, introduces a derogation system that is dependent on the purposes of processing.[419] Pursuant to art. 49(1)(a) GDPR, the data can be transferred after the data subject explicitly gave consent, or, pursuant to art. 49(1)(b) to(f) GDPR, the data can be transferred on the base of *necessity* for the performance or conclusion of a contract, for important reasons of public interest, for the establishment, exercise or defense of legal claims, or, in case the data subject is physically or legally incapable of giving consent, to protect the vital interests of the data subject or of other persons. The proportionality assessments that are embedded in the various references to *necessity* of processing rely for their lawful execution on purpose specification. This was discussed in Section 4.1.2.1.

Section 4.1.2.2 discussed *consent* in light of art. 6(1)(a) GDPR, which is only lawful when given for one or more purposes. This explicit connection does not exist between consent ex art. 49(1)(a) GDPR and the processing purposes of the data transfer. However, art. 4(11) defines consent of the data subject under the GDPR as any freely given, specific, informed and unambiguous indication of the data subject's wishes by which she, by a statement or by a clear affirmative action, signifies

[419] The derogation that is not dependent on processing purposes is art. 49(1)(g) GDPR: the personal data concerns semi-public information.

agreement to the processing of personal data relating to her.[420] This definition applies to all instances in which the GDPR requires *consent* of the data subject. As discussed in Section 4.1.2.2, the notion of *informed consent* in connection to the processing ground *consent* is explained in the Recitals of the GDPR as awareness of the data subject of at least the identity of the controller and the purposes of the processing for which the personal data are intended. Article 49(1)(a) GDPR requires *explicit* consent, which is explained by the EDPB[421] as "an express statement of consent", it is likely that this type of consent also requires awareness of the data subject of the processing purposes. The explicit purpose specification should, therefore, be communicated with the data subject in order to obtain lawful consent of the data subject.[422]

Article 49(1) GDPR introduces an additional derogation from the rules in art. 45 and 46 GDPR: when none of the exemptions of art. 49(1)(a)–(g) GDPR apply, the transfer to a third country or an international organization can still take place when it is not repetitive, concerns only a limited number of data subjects, and is necessary for the purposes of compelling legitimate interests pursued by the controller which are not overridden by the interests or rights and freedoms of the data subject. The controller should assess all the circumstances surrounding the data transfer and must provide suitable safeguards for the protection of personal data based on the outcome of the assessment.[423] The purpose specification requirement plays here a determinant role because the purposes are conditional for the prescribed proportionality test and the balancing of the interests of the data controller and the data subject.[424]

Under the LED purpose specification also plays an important role in data transfers in the absence of an adequacy decision[425] or appropriate safeguards.[426] As a general

[420] See also Section 3.5.2 on page 83.

[421] Article 29 Working Party *Guidelines on consent under Regulation 2016/679*, 2018. WP 259, p. 18.

[422] See to this extent also Article 29 Working Party *Guidelines on consent under Regulation 2016/679*, 2018. WP 259, p. 13. The EDPB formulated the minimum content requirements for consent to be *informed* and included the purpose of each of the processing operations for which consent is sought.

[423] Article 49(1) GDPR.

[424] Section 5.4.2 on page 179 details the characteristics of such a balancing test in the context of further use of personal data for incompatible purposes.

[425] The European Commission has the competence to determine, on the basis of article 45 GDPR whether a country outside the EU offers an adequate level of data protection. The effect of such an adequacy decision is that personal data can flow from the EU to that third country without any further safeguard being necessary. In others words, transfers to the country in question will be assimilated to intra-EU transfers of data.

[426] Article 46 GDPR.

rule competent authorities can only transfer data to a third country or an international organization for the objectives of the LED based on an adequacy decision of the Commission or appropriate safeguards.[427] However, in absence of these instruments data can still be transferred to a third country or an international organization under specific conditions, even if the purpose falls outside the scope of art. 1(1) LED. Pursuant to art. 38(1)(a)–(e) LED these transfers can only occur on the base of *necessity*, implying a proportionality test to which the processing purposes are conditional.[428]

The proportionality and necessity assessment for the lawful transfer of data to a third country or international organization in the absence an adequacy decision or appropriate safeguards, or other decision depend on the processing purposes.

4.1.3 Conditional for the application of data protection principles

This section will further investigate the role of the purpose specification requirement in data protection law and will contribute to the answer of the following subquestion: What is the relationship between the purpose specification requirement and the non-incompatibility requirement? As discussed in Section 3.5.1 on page 81, the purpose specification requirement is a component of the purpose limitation principle, which is one of the data protection principles. These principles also include the lawfulness, fairness and transparency principles, the non-incompatibility requirement of the purpose limitation principle, the data minimization-, accuracy-, and storage limitation principle, and the integrity and confidentiality principles. They are codified in art. 5(1) GDPR and art. 4(1) LED. The fundamental right to protection of personal data that is enshrined in art. 8 CFREU refers to the fairness- and lawfulness principle as well as the purpose specification requirement. This provision has been discussed in Section 2.1.2.4 on page 38.

All data protection principles depend on the purpose specification requirement in order to be applied and to have protective value for the rights of the data subject and instructive value for the obligations of the data controller. Because of this central role, the purpose specification requirement also becomes pivotal to the principle of accountability of the data controller, ex art. 5(2) GDPR and art. 4(4) LED.[429]

[427] Article 35(1)(a) LED; art. 36 and 37 LED; See Section 2.2.2.2 on page 53 for an discussion of the objectives of the LED.

[428] See Section 2.2.2.2 and 4.1.2.1.

[429] The EDPB also regards purpose specification a necessary condition for accountability. Article 29

4.1.3.1 Transparency, lawfulness and fairness

Transparency is considered an imperative for checks and balances of power in a democratic society. Public-private partnership could potentially undermine this legality mechanism through distributed and opaque data processing. The opacity of data processing increases in private-to-public data transfers when the quality of the data, the methodology and the quality of the technology that is used for data inferences are not communicated to the criminal law enforcement authority. The quality of the data can be expressed in the communication of the sources of the raw data, the accuracy of that data and whether or not the data is up-to-date. The communication of the methodology and applied technology for data inferences and probability calculations will reveal the trustworthiness of the inferences. In that case the private entity provides transparency with regard to the methodology and quality of the technology used for data inferences. This type of transparency can potentially function as a legality safeguard for public-private partnerships.[430]

Article 4(1)(a) LED, but also art. 28(1)(a) Europol Regulation, safeguard that Member States shall provide for personal data to be processed lawfully and fairly. The matching provision in the GDPR, article 5(1)(a), adds that personal data must be processed lawfully, fairly and *in a transparent manner* in relation to the data subject. The LED and the Europol Regulation only refer to *transparent processing* in their Recitals.[431] The Recitals of the LED explain that "any processing of personal data must be lawful, fair and transparent in relation to the natural persons concerned."[432] In general, transparency of processing is described as providing information on the existence of the processing, the identity of the controller and the purposes of the processing and further information to ensure fair and transparent processing.[433] The data subject must be given the opportunity to learn that personal data concerning her is collected, used, consulted or otherwise processed and to what extent the personal data is or will be processed.[434] This can partly be achieved by the communication of

Working Party *Opinion on Purpose Limitation*, 2013, WP 203, p. 13-15.

[430] Future research is needed to investigate the legality of public private partnerships in term of transparency of processing and data.

[431] In the Europol Regulation transparency is brought under the scope of fair processing, which "requires transparency of processing allowing data subjects concerned to exercise their rights." Recital 41 Europol Regulation.

[432] Recital 26 LED.

[433] Recital 39 GDPR; Recital 42 LED.

[434] Recital 60 GDPR; Data is oftentimes processed for multiple purposes and for every purpose the

the purpose specification in order to make the data subject and the supervisory authority understand the extent of the data processing and the risks that are involved.

Criminal law enforcement in a democratic society is characterized by the tension between transparency of government and secrecy in methods for effectiveness. The tools for balancing these competing interests must be provided for by law and the ECtHR has developed a set of minimum safeguards that have to be met by these laws in order to strike a fair balance between the legitimate aim pursued and the protection of fundamental rights, which will be discussed in Section 5.2.2.3.2 on page 166. The transparency principle is further detailed in data subject rights and data controller obligations which will be discussed in Section 4.1.4 and 4.1.5, where the dependency of the exercise of the transparency obligations and rights on the purposes of processing will be illustrated.

The fairness principle relates to the overall ingraining of the proportionality principle in the processing of personal data. Section 4.2 will discuss the contribution of the purpose specification requirement in the protection of fundamental rights and how it helps the execution of a proportionality assessment between the legitimate aim of restricting measures and the fundamental rights protection of those concerned. In order for processing to be fair, data subjects should be made aware of risks, rules, safeguards and rights in relation to the processing of personal data and how to exercise those rights.[435] This includes, for example, the requirement that a public administrative body informs the data subjects of the transfer of personal data to another public administrative body for the purpose of their processing by the latter in its capacity

obligation exists for the data controller to inform the data subject of the processing.When a controller intends to further process personal data for a purpose other than that for which the data was collected, art. 13(3) and art. 14(4) GDPR obligate the controller to provide the data subject with information on those secondary processing purposes together with any relevant further information prior to the secondary processing. The initial and new processing purposes are needed in order to audit if the processing purposes have changed at all. See also CJEU 1 October 2015, C-201/14 (*Smaranda Bara and Others*), par. 32, 40, 42-43. Purpose specification is, therefore, also conditional for the fulfillment of this information obligation. However, when the processing purposes do not or do no longer require the identification of a data subject by the controller, the data controller is released from the obligation to maintain, acquire or process additional information in order to identify the data subject for the sole purpose of complying with the GDPR ex art. 11(1) GDPR. This can include the dismissal from an obligation to process the data for an access and information request of the data subject. The processing purposes determine, therefore, the obligation to identify the data subject or not. See also Recital 57 GDPR.

[435] Recital 39 GDPR; recital 26 LED.

as recipient of those data.[436] In the field of criminal law enforcement the principle of fair processing embodies a distinct notion of the right to a fair trial as defined in art. 47 CFREU and in art. 6 ECHR.[437] These provisions apply when criminal charges are brought against an individual. In the *pre-crime* phase, which is the phase that is discussed in this study, these charges have not been brought and there is no guarantee that these charges will be brought against an individual at a later stage of the data processing. The safeguards that implement the right to a fair trial are therefore not applicable to the stage that this study focusses on: data transfers from private entities to criminal law enforcement authorities for the purpose of detection of crime. Nevertheless, once charges are brought the right applies retrospectively. Future research into the effects of this retrospective application on the legitimacy of public private partnerships in the pre-trial phase of criminal law enforcement is highly recommended.[438]

The lawfulness principle relates to the lawful processing grounds that form cumulative touchstones for lawful processing of personal data. Section 4.1.2 described the relationship between the processing grounds and the purpose limitation principle. The lawfulness of processing also connects with the broader idea of the Rule of Law, which was discussed in Section 3.4.2 on page 74, and the concept of *in accordance with the law* in fundamental rights protection.[439] The relationship between the purpose specification requirement and this concept will be discussed in Section 4.2.2 on page 119.

4.1.3.2 Accuracy of the data

The dependency of the accuracy principle on the purpose specification requirement is straightforward: Pursuant to art. 5(1)(d) GDPR and art. 4(1)(d) LED the processing purposes should be taken into account when the data is erased or rectified due to inaccuracy.[440] The accuracy principle is further detailed in the obligations for the

[436] CJEU 1 October 2015, C-201/14 (*Smaranda Bara and Others*), par. 34. See Section 4.1.1.2 on page 92 for a discussion on the implications of the qualification recipient and receiver of personal data and its effects on data controller obligations, including the obligation to inform, and data subject rights, including the right to information and access.

[437] Recital 26 LED.

[438] See Chapter 8.

[439] See to this extent also 3.5.3 on page 84.

[440] See also CJEU 16 December 2008, C-524/06, (*Huber/Germany*), par. 60.

data controller and the rights of the data subject which will be discussed in Section 4.1.4 and 4.1.5.

4.1.3.3 Non-incompatibility requirement

The non-incompatibility requirement is encapsulated in the second part of the purpose limitation principle and codified in art. 5(1)(b) GDPR and art. 4(1)(b) LED: Personal data must be collected for specified, explicit and legitimate purposes and not further processed in a manner incompatible with those purposes.[441] The non-incompatibility requirement is fully dependent on the purpose specification requirement. However, for its proper functioning the purpose specification requirement does not have a similar dependency on the non-incompatibility requirement, because it has protective value in data protection and fundamental rights law without being connected to use limitation based on the compatibility of purposes.[442]

4.1.3.4 Data minimization and storage limitation

Storage limitation and data minimization are principles that should be applied in relation to the processing purposes.[443] The engagement of the data minimization-, storage limitation- and the purpose limitation principle is illustrated by the findings of the EDPB in the *Opinion on the Application of Necessity and Proportionality Concepts and Data Protection within the Law Enforcement Sector* where the EPDB assessed the EU proposal on Smart Borders.[444] Purpose specification was used as a measure in the proportionality assessment for the effective implementation of the data minimization- and storage limitation principle in the data processing operations. The EDPB concluded that the objectives and purposes of the Smart Border proposal were insufficiently defined, leading to irrelevant and excessive personal data processing in violation of the data minimization and data accuracy principle.[445] Here, the neces-

[441] See Section 2.2 for more information on these instruments and other codifications of the non-incompatibility requirement.

[442] See chapter 5 to this extent. Further use based on the compatibility of purposes discussed in Section 5.1.

[443] See Section 3.5.1 on this topic.

[444] Article 29 Working Party *Opinion 05/2013 on Smart Borders*, 2013, WP 206, p. 10.

[445] See also Article 29 Working Party *Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector*, 2014, WP 221, p. 18.

sity question on *Should this data be processed?* could not be answered because the purposes were ill-defined.[446]

Article 5(1)(e) GDPR and art. 4(1)(e) LED require that personal data is kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed. The data minimization principle is codified in art. 4(1)(c) LED and art. 5(1)(c) GDPR. The latter two instruments require that personal data shall be adequate, relevant and *limited* to what is necessary in relation to the purposes for which they are processed. The provision on data minimization in LED speaks "adequate, relevant and *not excessive* in relation to the purposes for which they are collected and/or further processed", a phrasing that can also be found in the DPC.[447] This wording was previously also used in the Data Protection Directive, but got replaced by the more strict criterion of *necessity* with the adoption of the GDPR.[448] By replacing the negative construction of *not excessive* with the positive construction of *limited to what is necessary* in the GDPR, the EU legislature codified the interpretation of necessity by the CJEU in data protection matters.[449]

As already briefly stated in Section 3.5.1, the various data protection principles should be assessed in conjunction with one another. The *Digital Rights Ireland*-case and the *Tele2*-case illustrate this engagement. Those cases concerned legislative measures that ordered processing of personal data for ill-defined purposes and the failure to install the necessary safeguards in relation to these purposes.[450] In both cases the disputed measure did not require any relationship between the data which had to be retained and the objective of processing.[451] With regard to data minimization the

[446] See Section 4.1.2.1 on page 97 on the necessity questions in data protection law.

[447] Article 5(4)(c) DPC.

[448] Article 6(1)(c) DPD spoke of collection and/or further processing. Over the years this distinction became less relevant because collection constitutes data processing too.

[449] See for example CJEU 20 May 2003, joined cases C-465/00, C-138/01, C-139/01, (*Rechnungshof/Österreichischer Rundfunk and Others, and Christa Neukomm and Joseph Lauermann/Österreichischer Rundfunk*), par. 91; Why the EU legislature choose to adopt this doctrine only in the Regulations and not in the LED is to a large extent unclear, but could be attributed to the fact that the CJEU has not yet ruled on data processing matters in the field of criminal law enforcement and public security by competent authorities of Member States.

[450] See also: Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector, 2014, WP 221, p. 18; Article 29 Working Party *Opinion 05/2013 on Smart Borders*, 2013, WP 206, p. 19.

[451] CJEU 8 April 2014, joined cases C-293/12, C-594/12, (*Digital Rights Ireland Ltd/Ireland, and Kärntner Landesregierung/Michael Seitlinger, Christof Tschohl and others*), par. 59; CJEU 21 December 2016,

CJEU considered that the measures were not restricted to retention in relation to data pertaining to a particular time period and/or geographical area and/or a group of persons likely to be involved, in one way or another, in a serious crime, or persons who could, for other reasons, contribute, through their data being retained, to fighting crime.[452] In the *Tele2* case the CJEU underlined that in order to limit the retention to what is strictly necessary the data processing must continue to meet objective criteria that establish a connection between the data to be retained and the objective pursued.[453] The purpose specification requirement enables this proportionality assessment.[454] The processing purposes are, therefore, conditional for the implementation of data minimization and storage limitation in personal data processing.

4.1.4 Purposes (co-)determine the data subject rights

The data subject rights correspond with the high-level data protection principles. The type of processing purposes are conclusive in the application or revocation of some data subject rights. The following Sections discuss the data subject rights that are most dependent on the purposes specification requirement.

4.1.4.1 The right to erasure

The processing purposes are conditional for the scope and applications of the right to erasure. The connection between the right to erasure and the data protection principles was underlined by the CJEU in the *Google Spain*-case.[455] In that case the CJEU explained that data processing that violates data protection law "may result not only from the fact that such data are inaccurate but, in particular, also from the fact that they are inadequate, irrelevant or excessive in relation to the purposes of the processing, that they are not kept up to date, or that they are kept for longer than is necessary unless they are required to be kept for historical, statistical or scientific

C-203/15 and C-698/15 (*Tele2 Sverige/Post- och telestyrelsen* and *Secretary of State for the Home Department/Tom Watson, Peter Brice, Geoffrey Lewis*), par. 106.

[452] CJEU 8 April 2014, joined cases C-293/12, C-594/12, (*Digital Rights Ireland Ltd/Ireland, and Kärntner Landesregierung/Michael Seitlinger, Christof Tschohl and others*), par. 59.

[453] CJEU 21 December 2016, C-203/15 and C-698/15 (*Tele2 Sverige/Post- och telestyrelsen* and *Secretary of State for the Home Department/Tom Watson, Peter Brice, Geoffrey Lewis*), par. 110.

[454] CJEU 8 April 2014, joined cases C-293/12, C-594/12, (*Digital Rights Ireland Ltd/Ireland, and Kärntner Landesregierung/Michael Seitlinger, Christof Tschohl and others*), par. 63-64.

[455] CJEU 13 May 2014, C-131/12, (*Google Spain SL, Google Inc./AEPD, Mario Costeja González*).

purposes".[456] The CJEU pointed out that it follows from the data protection principles that even processing of data that was initially lawful may, in the course of time, become incompatible with the framework where those data are no longer necessary in the light of the purposes for which they were collected or processed.[457] The purpose specification requirement conditions, therefore, the exercise of the right to erasure of the data subject in the course of time.

Under the GDPR the data subject can exercise the right to erasure of personal data when the personal data are no longer necessary in relation to the purposes for which it was collected or otherwise processed or where the personal data have been unlawfully processed.[458] The LED obligates Member states to adopt legislation that forces the data controller to erase personal data where personal data is processed in violation of the data protection principles and rules regarding the lawfulness of processing.[459] As discussed in Section 4.1.2 and 4.1.3 the purpose specification requirement is of pivotal importance in determining the lawfulness of the processing and compliance with the data protection principles. Purpose specification is, therefore, an important factor in the exercise of this right under the GDPR and the LED.

Under the LED the data controller can restrict the data processing – instead of erase the personal data – when the data is necessary for the purposes of evidence.[460] Again, this rule depends on the purpose specification requirement.[461] Similarly, the right to erasure can be restricted under the GDPR when the personal data is processed for certain purposes, such as the processing for a purpose that falls under the scope

[456] CJEU 13 May 2014, C-131/12, (*Google Spain SL, Google Inc./AEPD, Mario Costeja González*), par. 92.

[457] CJEU 13 May 2014, C-131/12, (*Google Spain SL, Google Inc./AEPD, Mario Costeja González*), par. 93.

[458] 17(1)(a) and (d) GDPR. This provision also puts forward other situations in which personal data must be erased, but the purpose specification requirement does not play a central role in these other situations.

[459] Article 16(2) LED.

[460] Article 16(3)(b) LED; Also, under the LED Member States can pursuant to art. 16(4) LED, adopt legislative measures restricting, wholly or partly, the obligation to provide information on the refusal of erasure to the extent that such a restriction constitutes a necessary and proportionate measure in a democratic society with due regard for the fundamental rights and legitimate interests of the natural person concerned in order to for example avoid prejudicing the prevention, detection, investigation or prosecution of criminal offenses or the execution of criminal penalties, or to protect public security. To a certain extent the purposes of processing determine the scope of the right to be informed too.

[461] Another example is the influence of the processing purposes on the scope of the right of the data subject to have incomplete personal data completed, including by means of providing a supplementary statement. For the exercise of this right the processing purposes should be taken into account ex art. 16 GDPR and art. 16(1) LED. Article 16 GDPR and art. 16(1)LED and 47 LED.

of the right to freedom of expression and information or processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes when the erasure of data would render impossible or seriously impair the achievement of these objectives ex art. 17(3)(d) GDPR.[462]

4.1.4.2 Automated decision making

The purpose specification requirement directs the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning the data subject or similarly significantly affects her ex art. 22(1) GDPR. Pursuant to art. 22(2)(a) and (b) GDPR this right is not applicable when the decision is necessary for entering into or the performance of a contract between the data subject and a data controller, or when the decision is authorized by EU or Member State law. In both cases the explicit purpose specification is necessary to verify the applicability of these exemptions.

Furthermore, Article 22(2)(c) GDPR discharges the right that is laid down in art. 22(1) GDPR if the decision is based on the data subject's explicit consent. Contrary to some other provisions in the GDPR that refer to *consent*,[463] this provision lacks a direct reference of consent in relation to the purposes of processing. However, as discussed in Section 4.1.2.2, the conditions for *consent* to be informed include awareness of the data subject as to the purposes of the processing for which the personal data is collected.[464] The purpose specification requirement is therefore indirectly conditional for the appeal and execution of the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning her or similarly significantly affects her.[465]

[462] See Section 5.6 on the further processing of personal data for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes; See [Fazlioglu, 2013] on the tension between the data subject rights and the freedom of information online.; All data subject rights come with data controller obligations. Like this one: The obligation for the data controller to erase personal data that is no longer necessary to fulfill the processing purposes can be restricted ex art. 18(1)(c) GDPR in case the data subject needs the data herself for the purposes of the establishment, exercise or defense of legal claims. In this case the data will continue to be processed without the data controller being the identity that determines the processing purposes.

[463] Most notably art. 6(1)(a) and art. 9(2)(a) GDPR.

[464] Article 4(11) GDPR juncto Preamble 42 GDPR

[465] See art. 11 of the LED that contain the instructions for Member States regarding automated individual

4.1.4.3 The right to object

For data processing under the scope of the GDPR, the data subject has a right to object against the data processing that is dependent on the purpose specification requirement ex art. 21 GDPR. Where personal data processing is based on the legal grounds art. 6(1)(e) or (f) GDPR or the data is processed for direct marketing purposes the data subject has, ex art. 21(1) and (2) GDPR the right to object on grounds relating to her particular situation. This right includes the right to object against profiling based on these provisions. After receiving an objection from the data subject, the data controller is obligated to stop the data processing unless she demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or demonstrates that the data is processed for the establishment, exercise or defence of legal claims.

Following art. 22(6) GDPR the data subject also has the right to object on grounds relating to her particular situation in case personal data is processed for scientific or historical research purposes or statistical purposes. This right does not exist, however, where the processing is necessary for the performance of a task carried out for reasons of public interest. An explicit purpose specification is, therefore, necessary to verify wether or not the data is processed for direct marketing purposes, for scientific or historical research or statistical purposes, necessary for the performance of a task carried out for reasons of public interest, or necessary for the establishment, exercise or defense of legal claims. The explicit purpose specification is also necessary to execute the proportionality test between the compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject. It is safe to say that the application and scope of the right to object to processing of personal data is dependent on the processing purposes. An alternative model, such as replacing the purposes of processing with the interesest of the data controller, would not be suitable for this proportionality test.

decision-making. Other than a right to be informed ex art. 12 GDPR, there are no specific data subject rights connected to this provision.

4.1.5 Purposes (co-)determine the obligations for the data controller

The data subject rights that are described in Section 4.1.4 are mirrored by data controller obligations. For example, a successful appeal on the right to erasure of personal data results in the obligation for the controller to delete the personal data, and, if the data controller has made the personal data public, the obligation arises to inform other controllers that the data subject has requested the erasure of any copy of or link to the personal data.[466] There is, nevertheless, a set of data processing obligations that is independently applicable from the data subject rights. The most prominent of that group is the obligation to respect the data protection principles that is embedded in the accountability principle ex art. 5(2) GDPR and art. 4(4) LED. This obligation exists regardless of the substance of the processing purposes. Other data controller obligations in this set depend on the substance of the processing purposes for application. These obligations concern primarily concretizations of the general data controller obligation that forces the data controller to implement appropriate technical and organizational measures while taking into account the nature, scope, context and purposes of processing, as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons ex art. 24 GDPR and art. 19 LED.[467] This section focusses on this type of obligations.

4.1.5.1 Data protection by design

A result of the tightened regime on accountability for data controllers in European data protection law is the introduction of the notion of Data Protection by Design and by Default in the LED and GDPR.[468] The concept aims to ensure that privacy-related interests are neither forgotten nor marginalized in the initial design and subsequent development of information systems.[469] The impact of the obligation reaches beyond

[466] Article 17(2) GDPR; See Section 4.1.1.2 on the implications of the distiction recipient/receiver on obligation to notify other data controllers.

[467] See also recital 50 LED.

[468] The Europol Regulation only briefly refers to the notion of Data Protection by Design in art. 33 Europol Regulation: Europol shall implement appropriate technical and organizational measures and procedures in such a way that the data processing will comply with this Regulation and protect the rights of the data subjects concerned.

[469] [Bygrave, 2017, p. 106-107]; See also [Cavoukian et al., 2009]; The EDPB explained Data Protection by Design and by Default like this: a technical infrastructure that ensures, by default, that only those per-

its legal addressee, the data controller, because it has a so-called *up- and downstream effect*. Data Protection by Design and by Default is, in essence, directed towards data controllers, processors and system engineers.[470]

Article 25 GDPR and art. 19 LED prescribe a qualified duty for the data controller to take appropriate technical and organizational measures which are designed to implement the data protection principles in an effective manner.[471] Data protection by Design and by Default must be respected both at the time of the determination of the means for processing, and at the time of the processing itself. The provisions give guidance as to what circumstances should be recognized when considering the appropriateness of a measure. First the nature, scope, context and purposes of processing should be taken into account. Secondly, the fine line between *cutting edge technology* and *bleeding edge technology* has to be determined, as the data controller should assess *state of the art* solutions and the costs of their implementation. Lastly, the data controller must make a risk assessment taking into account the likelihood and the severity of interference with the rights and freedoms of natural persons posed by the processing. By referring to the rights and freedoms of natural persons – instead of the rights and freedoms of the data subject – the principle of DPbD forces the data

sonal data are processed which are necessary for each specific purpose of the processing and are especially not collected or retained beyond the minimum necessary for those purposes, both in terms of the amount of the data and the time of their storage. Article 29 Working Party *Opinion 07/2013 on the Data Protection Impact Assessment Template for Smart Grid and Smart Metering Systems ('DPIA Template') prepared by Expert Group 2 of the Commission's Smart Grid Task Force*, 2013, WP 209, p. 15; See also Article 29 Working Party *Opinion 02/2013 on apps on smart devices*, 2013, WP 202, p. 17.

[470] Recital 78 GDPR states: "When developing, designing, selecting and using applications, services and products that are based on the processing of personal data or process personal data to fulfill their task, producers of the products, services and applications should be encouraged to take into account the right to data protection when developing and designing such products, services and applications and, with due regard to the state of the art, to make sure that controllers and processors are able to fulfill their data protection obligations."

[471] The GDPR lists a few measures as examples of technical and organizational measures: pseudonymisation as soon as possible, minimizing the processing of personal data, transparency with regard to the functions and processing of personal data, enabling the data subject to monitor the data processing, enabling the controller to create and improve security features. Article 25(1) GDPR and Recital 78 GDPR. This list is not exhaustive. In de build-up to the coming into force of the GDPR, The European Union Agency for Network and Information Security (ENISA) released a report in which PETs are categorically described and connected to the data protection principles. See: *Privacy and Data Protection by Design – from policy to engineering*, ENISA, authors: Danezis, Domingo-Ferrer, Hansen, Hoepman, Metayer, Tirtea, and Schiffner, 2014.

controller to take a step back and assess the broader societal impact of the data processing. The processing purposes play an important role in this process, which makes the purpose specification requirement a precondition for the implementation of Data Protection by Design and by Default.

4.1.5.2 Data protection impact assessment

Following art. 35(1) GDPR and art. 27(1) LED the controller has the obligation to carry out a data protection impact assessment of intended personal data processing, when the type of data processing is likely to result in a high risk to the rights and freedoms of natural persons.[472] The processing purposes co-determine the necessity of the data protection impact assessment, and are a weighting factor in the impact assessment itself. This risk assessment should include the implication of the use of new technologies, and should take into account the nature, scope, context and purposes of the processing and mechanisms envisaged to ensure the protection of personal data and to demonstrate compliance with the data protection framework. Further down the line of a data protection impact assessment, the processing purposes serve as input to the assessment of the necessity and proportionality of the processing operations ex art. 35(7)(b) GDPR and art. 27(2) LED. The triggering and outcome of a data protection impact assessment is dependent on the processing purposes.

4.1.5.3 Security of processing

For the implementation of security measures the data controller and data processor have to take account of the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons ex art. 32(1) GDPR and art. 29(1) LED.[473] Under the Data Protection Directive the controller and processor had to take into account only the state of the art techniques and the cost of implementation while implementing appropriate technical and organizational measures to ensure a level of security appropriate to the risk of the data processing.[474]

[472] Recital 76 en 90 GDPR and Recital 58 LED.

[473] The Europol Regulation presents a more simple provision, that does not include a dependency on the processing purposes. See art. 32 Europol Regulation.

[474] CJEU 7 May 2009, C-553/07 (*Rijkeboer*), par. 62; CJEU 30 May 2013, C-342/12, (*Worten*), par. 24.

However, the CJEU has rejected financial considerations at the loss of strict security mechanisms due to a lack of sufficient safeguards to ensure effective protection of the data against the risk of abuse and against any unlawful access and use of personal data.[475] Following the footsteps of the CJEU, the EU legislature prescribed that the likelihood and severity of the risk of data processing should be assessed by looking at the nature, scope, context and purposes of the processing.[476] The purposes of processing are, therefore, a determinant in the risk assessment of the processing, and are central to the decision on the appropriateness of the security measures.[477]

4.1.5.4 Appointing a data protection officer and representative

For data processing under the scope of the GDPR, the controller and the processor are obligated to appoint a data protection officer when the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale.[478] Similarly, where data processing falls under the extraterritorial scope of the GDPR ex art. 3(2) GDPR, which was discussed in Section 2.2.2.1, the controller or the processor must designate in writing a representative in the EU ex art. 27(1). Data controllers or processors who are not established in the EU are dismissed from this obligation,[479] when the data processing is occasional, does not include, on a large scale, processing of special categories of data as referred to in art. 9(1) GDPR or processing of personal data relating to criminal convictions and offenses referred to in art. 10 GDPR, and is unlikely to result in a risk to the rights and freedoms of natural persons, taking into account the nature, context, scope and purposes of the processing. The processing purposes are therefore conditional for the decision on the appointment of a representative in the EU and a data protection officer.

[475] CJEU 8 April 2014, joined cases C-293/12, C-594/12, (*Digital Rights Ireland Ltd/Ireland, and Kärntner Landesregierung/Michael Seitlinger, Christof Tschohl and others*), par. 66 and 67.

[476] Recital 52 LED; Recital 90-94 GDPR.

[477] The integrity and confidentiality of personal data as well as the purpose specification requirement is considered by the CJEU to belong to the essence of the fundamental right to protection of personal data. See Section 4.2.4 on page 127.

[478] Article 37(1)(b) GDPR; Data processing in the field of criminal law enforcement requires a data data protection offer by default ex art. 32 LED and art. 40 Europol Regulation.

[479] Article 27(2)(a) GDPR.

4.1.5.5 Privileged purposes

Section 5.6 of this study describes the legal regime for the further processing of personal data for so-called *privileged purposes*, which are archiving purposes in the public interest, scientific and historical research purposes and statistical purposes in both the general and criminal law enforcement context.[480] When it comes to the role of purpose specification requirement, it is safe to say that the execution of this *lex specialis* rule is dependent on the purpose specification in order to verify if the processing indeed falls under this category of privileged purposes. The choices that have to be made regarding the implementation of data protection safeguards, and the lawfulness of restrictions on the data controller obligations and data subject rights when data is processed for privileged purposes are dependent on the processing purposes.[481] Personal data has to be, for example, pseudonymized or stripped from identifiers when the privileged purposes can be fulfilled in that manner.[482]

4.1.6 Conditional for the character of enforcement and proportionality of fining by the supervisory authority

The presence and quality of the explicit purpose specification influences the enforcement by the supervisory authority. This enforcement can be directed towards the obligations of the data controller that follow from the application of the purpose limitation principle itself to the data processing operations, but also towards obligations that follow from the other data protection rules that are dependent on the purpose specification requirements, as discussed in the previous Sections.[483] The supervisory authority has the obligation to respect the principle of proportionality whilst imposing administrative fines for infringements of the Regulation.[484] Pursuant to art. 83(2)(a) GDPR, when deciding in an individual case on imposition of such a fine and its sum, the supervisory authority should take into account the nature, gravity and duration of the infringement in light of the nature, scope and purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them. The purpose specification and processing purposes are via this provision also

[480] Article 4(3) and 9(2) LED; art. 5(1)(b) and 89 GDPR.
[481] See art. 89(2) and (3) GDPR.
[482] Article 89(1) GDPR.
[483] Article 83 GDPR.
[484] Article 83(1) GDPR.

a necessary factor to consider in the proportionality assessment of the enforcement decisions of the supervisory authority.

4.2 The purpose specification requirement and fundamental rights law

The previous sections of this chapter all investigated the subquestion: What is the role of the purpose specification in data protection law? This section takes a closer look at the fundamental rights restriction clauses in light of the purpose specification requirement.[485] The following subquestions are central in this section: "In what way is the idea behind purpose specification connected to the justification criteria of fundamental rights infringements?" and "To what extent is purpose specification connected to (the essence of) the fundamental right to respect for private life and the right to protection of personal data?"

Data transfers between private entities and competent authorities contain two data processing operations: the operation of disclosure the data by the private entity and the operation of receiving the data by the competent authority. In the introduction of this study the limitations to the scope of this study were explained.[486] The horizontal application of the rights secured in the ECHR is excluded from its scope. Section 2.1.1.4 described the criteria for vertical application of fundamental rights to data processing operations that are executed by private entities. Where the competent authority is highly engaged in the data processing operation of the private entity the data processing by the private entity falls under the accountability of the competent authority. Also, the Charter follows the scope of EU law. As illustrated in the *Google Spain*-case, the fundamental rights framework on protection of personal data and respect for private life is horizontally applicable.[487]

This chapter describes the justification criteria for interferences with the fundamental right to protection of personal data and the right to respect for private life. The rights protected in art. 8(1) ECHR can be restricted when the restricting measure

[485] See Section 5.2.2.3 for an investigation of these clauses in light of further use of data and the non-incompatibility requirement.

[486] See page 11.

[487] See in this regard also CJEU 13 May 2014, C-131/12, (*Google Spain SL, Google Inc./AEPD, Mario Costeja González*); See also 2.1.1 and 2.1.2.

pursues a legitimate aim, is in accordance with the law and is necessary in a democratic society pursuant to art. 8(2) ECHR. Any limitation on the exercise of the rights and freedoms recognized by the Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may only be made on the Charter rights if these are necessary and genuinely meet objectives of general interest recognized by the Union or the need to protect the rights and freedoms of others. These justification clauses can be summarized as the criteria of legitimate aim, legality, necessity and proportionality, and respect for the essence of the right. In the following three Sections the function of the purpose specification requirement is brought in connection with the first three criteria. The last Section focusses on the relationship between purpose specification and the notion of respect for the essence of the right.

4.2.1 Legitimate aim

The explicit purpose specification of a data processing operation that interferes with the fundamental rights can be indicative of the legitimate aim pursued. Article 8(2) ECHR includes an exhaustive list of legitimate aims, of which the most relevant ones for this study on the use of GDPR-data to detect and prevent crime are: national security, public safety and the prevention of disorder or crime. The restriction clause of the CFREU, art. 52(1), is less detailed and speaks of objectives of general interest recognized by the Union or the need to protect the rights and freedoms of others. Amongst these objectives of general interest, the CJEU has recognized the fight against international terrorism in order to maintain international peace and security,[488] the fight against serious crime in order to ensure public security,[489] as well as the prevention of offenses and the fight against crime, in particular organized crime.[490]

[488] CJEU 3 September 2008, C-402/05 and C-415/05 (*Kadi and Al Barakaat International Foundation/-Council and Commission*), par. 363; CJEU 15 November 2012, C-539/10 and C-550/10 (*Al-Aqsa/Council*), par. 130).

[489] CJEU 23 November 2010, C-145/09 (*Tsakouridis*), par. 46 and 47.

[490] CJEU 8 April 2014, joined cases C-293/12, C-594/12, (*Digital Rights Ireland Ltd/Ireland, and Kärntner Landesregierung/Michael Seitlinger, Christof Tschohl and others*), par. 43. The indicative function of the explicit purpose specification in the determination of the legitimate aim of restricting measures has been underlined by the EDPS in a special developed toolkit for the assessment of the necessity of measures that interfere with the fundamental right to protection of personal data; EDPS, 11 April 2017, *Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit*, p. 15.

4.2.2 Legality

The element of legitimate purposes connects to the criterion *in accordance with the law* as both concepts require compatibility with the Rule of Law.[491] The case law that is discussed in this Section makes (in)direct references to the ideal of the Rule of Law, which demands boundaries on and clarity of competence to restrict power.[492] These boundaries can be set by purpose specification in legislative measures that foresee in the interferences. Here the distinction must be made between the codification of the explicit purpose specification and the codification of the purpose specification requirement. Codification of the latter does not render a measure *in accordance with the law*. The criterion *in accordance with the law* includes the quality of the law, which concerns the accessibility and foreseeability of a restricting measure, as well as the existence of necessary procedural safeguards that provide adequate legal protection against arbitrary application of the measure.[493]

This distinction became clear in the *Amann*-case, that concerned a disputed measure which contained rules applicable to the processing of personal data by the federal administration in Switzerland.[494] These rules consisted of general principles, including a purpose specification provision that stated "personal data may be processed only for very specific purposes". The ECtHR did not regard these general principles as appropriate indications of the scope and conditions of the exercise of power that was conferred on the competent authorities to gather, record and store information.[495] The rules lacked specificity and for this reason the ECtHR considered the data protection rules and the general mandate of the federal administration not sufficiently clear and detailed to guarantee adequate protection against interference by the authorities with the right to respect for private life.[496] In other words: the restricting measures

[491] This criterion is discussed in light of further use of personal data and the non-incompatibility requirement in Section 5.2.2.3.2 on page 162. See also Section 3.4.2 on page 74.

[492] See for example ECtHR 25 March 1983, no. 5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75, 7136/75) (*Silver and Others/the United Kingdom*), par. 34; ECtHR 2 Augustus 1984, no. 8691/79 (*Malone/the United Kingdom*) par. 67.

[493] ECtHR 25 June 1997, no. 20605/92 (*Halford/the United Kingdom*), par. 49; ECtHR 25 March 1983, no. 5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75, 7136/75) (*Silver and Others/the United Kingdom*).

[494] ECtHR 16 February 2000, no. 27798/95 (*Amann/Switzerland*).

[495] ECHR. ECtHR 16 February 2000, no. 27798/95 (*Amann/Switzerland*), par. 76-78.

[496] The processing of the data that related to the private life of the applicant was therefore not in accordance with the law and violated art. 8 ECHR. ECtHR 16 February 2000, no. 27798/95 (*Amann/Switzer-*

lacked explicit purpose specification that accompanied the data processing powers.

The *Malone*-case also illustrates how the ECtHR found a violation of art. 8 ECHR because the domestic law governing the processing of data for police purposes was "somewhat obscure and open to differing interpretations".[497] On the evidence before the ECtHR it could not be said with any reasonable certainty what elements of the powers to collect data were incorporated in legal rules and what elements remained within the discretion of the executive.[498] As a result of this obscurity and uncertainty, the ECtHR concluded that the domestic law did not indicate with reasonable clarity the scope and manner of exercise of the relevant discretion conferred on the public authorities when it collected data based on the disputed powers.[499] When looking at this case from a data protection in stead of criminal law point of view, the ECtHR's considerations translate to the demand to, firstly, codify the objectives for which the powers can be authorized, and, secondly, to specify the processing purposes of the concrete data processing operation prior to the authorization of the restricting measure.

The CJEU connected the requirement of foreseeability, which in itself in connected to the criterion of quality of the law, to the purpose specification requirement in the *Österreichischer Rundfunk*-case.[500] In that case the CJEU investigated the explicit purpose specification that was embedded in a legal provision.[501] The CJEU explained that the processing purposes have to be legitimate, formulated with sufficient precision and accessible to enable individuals to adjust their conduct accordingly.[502]

land), par. 76-78.

[497] ECtHR 2 Augustus 1984, no. 8691/79 (*Malone/the United Kingdom*), par. 67-80.

[498] ECtHR 2 Augustus 1984, no. 8691/79 (*Malone/the United Kingdom*), par. 67-80; Text inspired on ECtHR 13 November 2012, no. 24029/07 (*M.M./the United Kingdom*), par. 194.

[499] ECtHR 2 Augustus 1984, no. 8691/79 (*Malone/the United Kingdom*), par. 69-80; See also ECtHR 26 March 1987, no. 9248/81, (*Leander/Sweden*) par. 50.

[500] CJEU 20 May 2003, joined cases C-465/00, C-138/01, C-139/01, (*Rechnungshof/Österreichischer Rundfunk and Others, and Christa Neukomm and Joseph Lauermann/Österreichischer Rundfunk*).

[501] CJEU 20 May 2003, joined cases C-465/00, C-138/01, C-139/01, (*Rechnungshof/Österreichischer Rundfunk and Others, and Christa Neukomm and Joseph Lauermann/Österreichischer Rundfunk*), par. 76-78.

[502] CJEU 20 May 2003, joined cases C-465/00, C-138/01, C-139/01 (*Rechnungshof/Österreichischer Rundfunk and Others, and Christa Neukomm and Joseph Lauermann/Österreichischer Rundfunk*) par. 77. See to this extent also the Opinion of the Advocate General in the *Promusicae*-case that was discussed in Section 3.5.3 of this study. The A-G connected the criterion of foreseeability to art. 8(2) CFREU and explained that the requirement of foreseeability has found particular expression in data protection law in the criterion – expressly mentioned in Article 8(2) of the Charter – of purpose limitation. Opinion A-G, CJEU 18 July 2007, C-275/06 (*Productores de Música de España (Promusicae)/Telefónica de España*

The ECtHR's and the CJEU both connected the objectives of processing and the processing purposes to the criterion of foreseeability and the legality of processing. The purpose specification requirement contributes to the quality of the law that is required by art 8(2) ECHR and art. 52(1) CFREU for measures that infringe on the fundamental rights.[503]

4.2.3 Necessity and proportionality

The next step in the assessment of the justification of an infringement covers necessity criterion, which also includes the subsidiarity assessment of the measure, and proportionality of the restricting measure. In section 4.1.2.1 on page 97 I discussed necessity in light of data protection regulation. Restrictions on the fundamental rights are only legitimate in so far as these are strictly necessary.[504] The subsidiarity of a measure looks after the existence of alternative less-infringing means to accomplish the legitimate aim pursued. [505] The proportionality criterion limits the authorities in the exercise of their powers by requiring a balance to be struck between the means used and the intended aim.

The concepts of necessity and proportionality in data protection cases are fact-based concepts, which must be assessed in light of the circumstances of the case, the provisions of the measure and the concrete purpose it aims to achieve.[506] The

SAU), par. 53. The CJEU did not discuss these aspects in its judgement. See CJEU 29 January 2008, C-275/06, (*Productores de Música de España (Promusicae)/Telefónica de España SAU*); See [Kuner, 2008] and [Coudert and Werkers, 2008] that discuss the balancing of copyright interests and privacy rights.

[503] See also Section 5.2.2.3.2 of this study.

[504] CJEU 19 November 2010, C-92/09 and C-93/09, (*Volker and Markus Schecke and Eifert*), par. 77 and 86; CJEU 16 December 2008, C-73/07, (*Tietosuojavaltuutettu/Satakunnan Markkinapörssi Oy and Satamedia Oy*), par. 56; ECtHR 29 April 2014, no. 52019/07 (*L.H./Latvia*); ECtHR 29 June 2006, no. 54934/00 (*Weber and Saravia/Germany*); ECtHR 4 December 2015, no. 47143/06 (*Roman Zakharov/Russia*.

[505] The advocate- General in the Huber-case explained that the authority adopting a measure which interferes with a right protected by Community law in order to achieve a legitimate aim must demonstrate that the measure is *the least restrictive* for the achievement of this aim. Opinion A-G, CJEU 3 April 2008, C-275/06, (*Huber/Germany*), par. 27; See also CJEU 16 July 2015, C-83/14, (*CHEZ Razpredelenie Bulgaria AD/Komisia za zashtita ot diskriminatsia*), par. 123.

[506] CJEU 20 May 2003, joined cases C-465/00, C-138/01, C-139/01, (*Rechnungshof/Österreichischer Rundfunk and Others, and Christa Neukomm and Joseph Lauermann/Österreichischer Rundfunk*), par. 75; CJEU 8 April 2014, joined cases C-293/12, C-594/12, (*Digital Rights Ireland Ltd/Ireland, and Kärntner Landesregierung/Michael Seitlinger, Christof Tschohl and others*), par. 33; ECtHR 4 December 2008, no.130562/04 and 30566/04 (*S. and Marper/the United Kingdom*), par. 67.

EDPB explained that "From a privacy perspective failure to tightly define the purpose for processing personal data will mean that the pressing social need is insufficiently defined."[507] Necessity implies the need for a combined, fact-based assessment of the effectiveness of the measure for the objective pursued.[508] The EDPS explained that testing the necessity of the measure is the first step in this assessment and that when the measure does not pass the necessity test, there is no need to examine its proportionality.[509] This connects to the first out of three necessity and proportionality questions that were identified on page 97 in the context of data protection law. When there is no need to process personal data because the processing purpose can be fulfilled with the processing of other information, there is no need to answer question two and three on the subsidiarity and proportionality.

The case law of the CJEU and ECtHR shows a less structured assessment that frequently shifts back and forth between the assessment of the necessity and appropriateness, and assessment of the proportionality. However, some of the steps of the assessment and notions are settled. According to the ECtHR's settled case-law, the notion of necessity implies that the interference with the right to respect for private life corresponds to a pressing social need, and that the interference is proportionate to the legitimate aim pursued.[510] For this assessment the ECtHR considers if the reasons adduced for justification of the interference are relevant and sufficient in the light of the case as a whole.[511] This includes the nature, scope and duration of the possible measures, the grounds required for ordering them, the authorities competent to authorize, carry out and supervise them, and the kind of remedy provided by the national law.[512] In this context the ECtHR has occasionally called for data protection

[507] Article 29 Working Party *Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector*, 2014, WP 221, p. 19.

[508] EDPS, 11 April 2017, *Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit*, p. 5.

[509] EDPS, 11 April 2017, *Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit*, p. 4.

[510] ECtHR 30 October 2012, no. 57375/08 (*P. and S./Poland*), par. 94; See Section 5.2.2.3.1 in page 160 for a discussion of the requirement of legitimate aim.

[511] ECtHR 28 January 2003, no. 44647/98 (*Peck/the United Kingdom*) par. 76; ECtHR 26 January 2017, no. 42788/06 (*Surikov/Ukrain*), par. 73; acsECtHR 18 May 2010, no. 26839/05 (*Kennedy/the United Kingdom*), par. 154; ECtHR 29 June 2006, no. 54934/00 (*Weber and Saravia/Germany*), par. 106; ECtHR 4 December 2015, no. 47143/06 (*Roman Zakharov/Russia*), par. 233.

[512] See for example ECtHR 6 September 1978, no. 5029/71 (*Klass and others/Federal Republic of Germany*), par. 50; See for a compact and straightforward assessment ECtHR 2 September 2010, no. 35623/05

safeguards, such as proportional data minimization, and anonymisation in relation to the processing purposes and impact of the interference.[513] In the *Gardel*-case, for example, the ECtHR stressed that the need for such safeguards is all the greater where personal data is undergoing automatic processing, not least when such data are used for police purposes.[514] With a reference to the DPC[515] and CoE R(87) 15,[516] the ECtHR explained that in order for the processing to be necessary in a democratic society, the domestic law should ensure that the data is relevant and not excessive in relation to the purposes for which it is stored, and that the data is preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which the data is stored.[517] The execution of these safeguards that justify interferences on fundamental rights are dependent on the processing purposes.

Closely connected to the doctrine developed by the ECtHR is the interpretation of the principle of proportionality by the CJEU, which requires that legislation is appropriate for attaining the legitimate objectives pursued by the legislation at issue and do not exceed the limits of what is appropriate and necessary in order to achieve its objectives.[518] According to the CJEU's settled case-law, limitations on the rights protected in art. 7 and 8 CFREU should apply only in so far as is strictly necessary and with respect for the principle of proportionality.[519] In the *Schrems*-case, for example, the CJEU explained that legislation should be limited to what is strictly necessary by means of objective criteria to determine the limits of access and of its subsequent use, for purposes which are specific, strictly restricted and capable of jus-

(*Uzun/Turkey*), par. 80.

[513] See for example ECtHR 6 June 2016, no.37138/14 (*Szabó and Vissy/Hungary*), par. 73; ECtHR 4 December 2015, no. 47143/06 (*Roman Zakharov/Russia*), par. 249.

[514] ECtHR 17 December 2009, no. 16428/05 (*Gardel/France*), par. 62.

[515] See Section 2.2.1.1 on page 47 for a discussion of the DPC.

[516] See Section 2.2.1.2 on page 48 on the Recommendation (87) 15 on Regulating the Use of Personal Data in the Police Sector.

[517] ECtHR 17 December 2009, no. 16428/05 (*Gardel/France*), par. 62.

[518] CJEU 8 April 2014, C-293/12 and C-594/12, (*Digital Rights Ireland*) par. 46; CJEU 19 November 2010, C-92/09 and C-93/09, (*Volker and Markus Schecke and Eifert*) par. 74.

[519] See Section 2.1.2.5 on the relationship between art. 7 and 8 CFREU; CJEU 19 November 2010, C-92/09 and C-93/09, (*Volker and Markus Schecke and Eifert*) par. 77; CJEU 8 April 2014, C-293/12 and C-594/12, (*Digital Rights Ireland*) par. 52; CJEU 8 October 2015, C-362/14 (*Schrems*), par. 92; CJEU 16 December 2008, C-73/07, (*Tietosuojavaltuutettu/Satakunnan Markkinapörssi Oy and Satamedia Oy*), par. 56; CJEU 7 November 2013, C-473/12, (*IPI*), par. 39; CJEU 21 December 2016, C-203/15 and C-698/15 (*Tele2 Sverige/Post- och telestyrelsen* and *Secretary of State for the Home Department/Tom Watson, Peter Brice, Geoffrey Lewis*), par. 96.

tifying the interference made by the access to the data and its further use with the fundamental right to respect for private life.[520] In these paragraphs the CJEU underlines the autonomous function of the purpose specification requirement, but also made the requirement conditional to the proportional application of other data protection safeguards for the protection of fundamental rights.[521] The CJEU highlights that safeguards can be provided by data minimization, access regulation, use limitation and storage limitation *in relation to the purposes of processing*.[522] The purpose specification requirement is, therefore, conditional for the application of the necessity and proportionality test in data processing cases that concern fundamental rights infringements.

4.2.4 Respect for the essence of the fundamental right to protection of personal data

The previous sections discussed the function of the purpose specification requirement in relation to the criteria of legitimate aim, legality, and necessity and proportionality in fundamental rights law. This section investigates the relationship of the purpose specification requirement and the criterion of *respect for the essence of the right* that has been laid down in art. 52(1) CFREU.[523] An interference with the essence of the

[520] CJEU 8 October 2015, C-362/14 (*Schrems*), par. 93-94.

[521] CJEU 8 October 2015, C-362/14 (*Schrems*) par. 93 and 94.

[522] CJEU 8 October 2015, C-362/14 (*Schrems*) par. 93 and 94; See also CJEU 8 April 2014, joined cases C-293/12, C-594/12, (*Digital Rights Ireland Ltd/Ireland, and Kärntner Landesregierung/Michael Seitlinger, Christof Tschohl and others*), par. 60 and 61; CJEU 21 December 2016, C-203/15 and C-698/15 (*Tele2 Sverige/Post- och telestyrelsen* and *Secretary of State for the Home Department/Tom Watson, Peter Brice, Geoffrey Lewis*) par. 118.

[523] Until recently this criterion was preserved to the jurisdiction of the EU, but after the revision of the DPC in 2013, the restriction clause of that data protection treaty incorporated the criterion too, illustrating the ongoing dialogue between the jurisdiction of the Council of Europe and the European Union about fundamental rights protection. The DPC secures that, pursuant to art. 11(1)(a) DPC, restrictions on the non-incompatibility requirement ex art. 5(4)(b) DPC are only allowed when the restricting measure is provided for by law, respects the essence of the fundamental rights and freedoms and constitutes a necessary and proportionate measure in a democratic society for a specific legitimate aim, which includes the investigation and prosecution of criminal offenses, national security and public safety. See also Section 4.1.2.3 on page 98; Article 52(1) CFREU should be read in the tradition of respect for the *very substance of a fundamental right*, an expression deployed by the CJEU before the adoption of the CFREU. This expression stems from doctrine in which the exercise of some fundamental rights could be restricted, provided that the restrictions in fact correspond to objectives of general interest and are not – taking into account of the

right cannot be balanced away by other legitimate societal or general interests, or the rights and freedoms of others. Once a measure violates the essence of a right, its future deployment is off the table, regardless of increased societal or general interests, even if these interests are, as such, very weighty, like an imminent threat of terrorism.

The essence of the essence of the right is highly debated amongst legal scholars. Brkan argues, for example, that the essence of a fundamental right can be breached in many different circumstances, which results in many possible *essences* of one fundamental right.[524] Ojanen, on the other hand, leans towards one essence for every right.[525] When looking at the case law of the CJEU on data protection it appears that, rather than describing the essence of a right in terms of *objectives* that may be pursued, the CJEU describes the essence of the right in terms of the *means* that have to be put in place to safeguard the minimum level of protection of personal data.[526] Data protection principles are put forward by the CJEU as means of protection. This results in a core set of principles that have to be observed in order to respect the essence of the fundamental right to protection of personal data.[527] This core set of principles includes the purpose specification requirement.

The *essence of the right* is discussed by the CJEU in three cases that concerned the processing of personal data. First, in the *Digital Rights Ireland*-case the CJEU explained that the retention of personal data, including telecommunication metadata, did not compromise the essence of the right to private life art. 7 CFREU, because the Directive did not permit the acquisition of knowledge of the content of the electronic communications.[528] The essence of the right to protection of personal data ex art. 8 CFREU was also not compromised because the data controller had to respect certain principles of data protection and data security, that secured appropriate technical and organizational measures against accidental or unlawful destruction, accidental loss or alteration of the data.[529] Traditionally, the idea of confidentiality is connected to

aim of the restrictions – disproportionate and unacceptable by impairing the *very substance of the rights* guaranteed. See for example CJEU 12 June 2003, C-112/00,*Schmidberger, Internationale Transporte und Planzüge*) par. 80. Occasionally the CJEU still refers to *the very substance of the right*. See for example CJEU 26 September 2013, C 418/11 (*Texdata Software*), par. 71-77 and 84.

[524] [Brkan, 2017, p. 14].

[525] [Ojanen, 2016, p. 326].

[526] Similarly [Lynskey, 2015, p. 171].

[527] See also [Brkan, 2019] on the essence of the fundamental rights to privacy and data protection.

[528] CJEU 8 April 2014, C-293/12 and C-594/12, (*Digital Rights Ireland*), par. 39.

[529] CJEU 8 April 2014, C-293/12 and C-594/12, (*Digital Rights Ireland*), par. 40.

communication, which is just one of many potential objectives of data processing. In the *Digital Rights Ireland*-case the CJEU began to approach confidentiality as a characteristic of technical infrastructures, which are the *means* of data processing.[530] This case started to put forward an important role for the integrity and confidentiality principle in light of the essence of the right to protection of personal data.

Another critical case that concerned respect for the essence of the right in data processing operations is the *Schrems*-case.[531] The Advocate-General in that case questioned whether the limitations at issue had to be regarded as respecting the essence of art. 7 and 8 CFREU because of the access by a third country to the transferred data seemed to extend to the content of the electronic communications.[532] The Advocate General regarded this as compromising the essence of the fundamental right to respect for privacy ex art. 7 CFREU. The CJEU partly copied this advice and underlined that legislation permitting the public authorities to have access on a generalized basis to the content of electronic communications must be regarded as compromising the essence of the fundamental right to respect for private life, as guaranteed by art. 7 CFREU.[533] The Advocate General also commented on the respect for the essence of the fundamental right to protection of personal data, but this point was not picked up by the CJEU.[534]

The last important case is the *Canada-EU PNR*-opinion[535] of the CJEU, in which the essence of the fundamental right to protection of personal data was elaborated on by the Advocate General and briefly touched upon by the Grand Chamber of the CJEU.[536] The Advocate-General took the nature of the data as a starting point and explained that the data processing pursuant to the PNR agreement does not permit any precise conclusions to be drawn as regards the *essence of the private life* of the persons

[530] See a discussion on this aspect in European Human Right Cases 2014/140, M.E. Koning, *Annotation to CJEU Digital Rights Ireland, C-293/12 and C-594/12*, par. 14

[531] CJEU 8 October 2015, C-362/14 (*Schrems*).

[532] Opinion A-G, CJEU 23 September 2015, C-362/14, (*Schrems*), par. 177.

[533] CJEU 8 October 2015, C-362/14 (*Schrems*), par. 94.

[534] The A-G noted that "since the broad wording of the limitations provided for in the fourth paragraph of Annex I to Decision 2000/520 potentially allows all the safe harbor principles to be disapplied, it could be considered that those limitations compromise the essence of the fundamental right to protection of personal data." Opinion A-G, CJEU 23 September 2015, C-362/14, (*Schrems*), par. 177.

[535] Passenger Name Records.

[536] Opinion CJEU (Grand Chamber), 26 July 2017, ECLI:EU:C:2017:592, (*Opinion on the Draft Agreement between Canada and the European Union 1/15*); Opinion A-G, 8 September 2016, ECLI:EU:C:2016:656, (*Opinion on the Draft Agreement between Canada and the European Union 1/15*).

concerned, because it only concerns the pattern of air travel of passengers between Canada and the EU.[537] The CJEU copied this starting point and explained that "even if PNR data may, in some circumstances, reveal very specific information concerning the private life of a person, the nature of that information is limited to certain aspects of that private life, in particular, relating to air travel between Canada and the European Union."[538] With regard to the essence of the right of the protection of personal data, the Advocate General noted that Canada is required, in particular, to "ensure compliance verification and the protection, security, confidentiality and integrity of the data," and also has to implement "regulatory, procedural or technical measures to protect data against accidental, unlawful or unauthorized access, processing or loss".[539] The Grand Chamber observed that the envisaged agreement limits the purposes for which the personal data may be processed and lays down rules intended to ensure, inter alia, the security, confidentiality and integrity of that data, and to protect it against unlawful access and processing.[540] The integrity and confidentiality principle and the purpose specification requirement are connected to the protection of the essence of the right by the CJEU.[541]

From the case law the following conclusion can be drawn: The essence of the right to respect for private life can be revealed by looking at the *essence of private life* which is the objective of the protection of art. 7 CFREU. This essence excludes at least access of the government to the content of communication in a generalized manner and the possibility to make precise conclusions about a person's private life in a generalized

[537] Opinion A-G, 8 September 2016, ECLI:EU:C:2016:656, (*Opinion on the Draft Agreement between Canada and the European Union 1/15*) par. 186. To this regard the Advocate General took into account the data protection provisions of the PNR agreement that guarantee the masking and gradual depersonalization of the personal data that is processed.

[538] Opinion CJEU (Grand Chamber), 26 July 2017, ECLI:EU:C:2017:592, (*Opinion on the Draft Agreement between Canada and the European Union 1/15*), par. 150.

[539] Opinion A-G, 8 September 2016, ECLI:EU:C:2016:656, (*Opinion on the Draft Agreement between Canada and the European Union 1/15*) par. 187.The fact that the PNR agreement also secures that any breach of data security must be amenable to effective and dissuasive corrective measures which might include sanctions, was also regarded by the Advocate General to contribute positively to the protection of fundamental rights.

[540] Opinion CJEU (Grand Chamber), 26 July 2017, ECLI:EU:C:2017:592, (*Opinion on the Draft Agreement between Canada and the European Union 1/15*), par. 150.

[541] In Section 4.1.5.3 on page 114 highlighted the dependency of the proper implementation of security measures on the purposes of processing. To this extent we see that the multiple facets of the essence of the right to protection of personal data also show interdependency towards each other.

manner. The essence of the right to protection of personal data entails the minimum means that have to be put in place to enjoy effective protection of personal data. The case law discussed in this Section suggests that these means include at least the safeguarding of the integrity and confidentiality of personal data and the purpose specification requirement.

Based on the *Canada-EU PNR*-opinion of the CJEU, some scholars claim that the full purpose limitation principle – meaning the purpose specification requirement and the non-incompatibility requirement – belongs to the essence of the fundamental right to protection for personal data, which leads to problematic analyses of further use of, for example, GDPR-data for LED purposes.[542] I disagree with these scholars. I believe that only the purpose specific requirement belongs to the essence of the right for two reasons.

First, as explained on page 125, the essence of the right consists of the core of a fundamental right on which any limitation results in a violation that can never be justified, regardless of changing circumstances, such as a greater pressing social need. European secondary data protection law presents a well-balanced system of derogations on the non-incompatibility requirement which is either based on renewed consent or on a *lex specialis* that meets the criteria of legality, legitimate aim, and necessity and proportionality, which will be discussed in Section 5.2.2, 5.3 and Section 5.5. If the non-incompatibility requirement were part of the essence of the right, such derogations would be in violation with fundamental rights protection. Also, Section 5.1.2.2 will show that the CJEU ruled on multiple cases that concerned the further processing of data for incompatible purposes without even noticing that the non-incompatibility requirement was at stake.

The second reason relates to the distinctly different function that the purpose specification requirement fulfills in data protection and fundamental rights law compared to the function of the non-incompatibility requirement. As will be discussed in chapter 5, the non-incompatibility requirement is one out of various methods to limit the further use of personal data, whereas in this chapter I have argued that the purpose specification requirement fulfills a conditional function on which the proper functioning of the whole legal framework depends. The purpose specification requirement ties together the whole data protection and fundamental rights framework and the

[542] See for example [Jasserand, 2018, p. 160].

processing purposes are a necessary precondition in order to apply the other data protection safeguards.

For these reasons I argue that purpose specification is part of the essence of the right to protection of personal data, and the non-incompatibility requirement or any other type of use limitation is not.

4.3 Conclusion on the purpose specification requirement

With regard to the role of the purpose specification requirement in data protection law, this chapter has shown that this requirement is a central concept in data protection law. The purpose specification requirement has an independent role in data protection that is not necessarily connected to the non-incompatibility requirement.

Through its conditional function it is directly and indirectly connected to other pivotal data protection concepts and rules. Direct dependency exists for the data protection principles that can only function as a whole set and depend on the status of the requirement as a data protection principle. Indirect dependency on the purpose specification requirement exist when rules, rights and obligations are dependent on the purpose specification or on the processing purposes for their applicability, application and outcome. The various necessity and proportionality assessments that are embedded in data protection law are indirectly dependent on the purpose specification requirement. This dependency on the purpose specification requirement extends to the application of the other data protection principles, the lawfulness of the application of the legitimate processing grounds and the application and execution of the new data controller accountability obligations, such as a data protection impact assessments.

We saw that the non-incompatibility requirement is dependent on the purpose specification requirement for its functioning and effect, but that the purpose specification requirement does not have a similar depending relationship with the non-incompatibility requirement. Also, other forms of use limitation, such as the further use rules under the LED, are dependent on the purpose specification requirement. The application and scope of some of the data subject rights and data controller obligations are dependent on the purposes of processing. As a result of the conditional

function of the purpose specification requirement, erosion of the conception of purpose limitation results in the erosion of all related data protection principles and rules, and has effect on data protection as a whole, including the fundamental right to protection of personal data.

In the case law of the ECtHR on data processing, purpose limitation makes no explicit appearance, but plays, nevertheless, an ominous yet delicate role in the justification of an infringement on the right to respect for private life. Both the CJEU and the ECtHR pay special attention to the purpose specification requirement in their case law. The purpose specification requirement is connected to all the justification criteria in fundamental rights law. It is taken into account at all three stages of the triple test, that defines the justification of fundamental rights infringements. The *legitimate aim* of an interference is different from the processing purposes. Yet, this chapter has shown that the latter will oftentimes function as a starting point for the assessment of the legitimate aim of a restricting measure for the European courts. The criterion *in accordance with the law* includes the quality of the law, which concerns the accessibility and foreseeability of a restricting measure, as well as the existence of necessary procedural safeguards that provide adequate legal protection against arbitrary application of the measure. The criterion in accordance with the law refers to the rule of law, meaning that an infringing measure should be based on accessible, foreseeable law that is encompassed with safeguards. Overall, the purpose specification requirement is necessary for the execution of the general requirement of proportionality of data processing and the requirement functions as a safeguard.

The most significant finding of all this is that the purpose specification requirement plays an essential autonomous and conditional role in the protection of personal data and should be considered as belonging to the essence of the fundamental right to protection of personal data. All limitations on the rights protected in the CFREU must respect the essence of these rights. Limitations on the purpose specification requirement rip away the protection from the carefully build up data protection and fundamental rights law framework, and are therefore prohibited.

Chapter 5

Limitations on the use of personal data

This Chapter discusses the various way in which personal data processing is limited under European data protection and fundamental rights law. In Chapter 3 a general description of the role of the non-incompatibility requirement has been given. In this chapter we will go in more detail in order to determine the role of the non-incompatibility requirement in data protection and fundamental rights law. Here, the relationship of the two requirements of the purpose limitation principle will become more clear. The other types of use limitation in data protection law will be investigated as well as their relationship with the non-incompatibility requirement.

5.1 Further processing based on compatibility between purposes

The first type of use limitation that is discussed in this study is based on the compatibility between the initial and new processing purposes, which is regulated by the non-incompatibility requirement. That requirement is part of the purpose limitation principle, as discussed in Chapter 3 and is included in all the investigated data protection law as described in Section 2.1.

5.1.1 The compatibility test

The purpose limitation principle obligates the data controller to perform a compatibility test. Section 3.3.6 on page 71 described the factors that should be taken into account for such an assessment. The compatibility assessment includes an assessment of the similarity of the initial purposes and the new purposes. In first step the focus should be on the purposes and not on the objectives, field or context of processing.

This is specifically important for processing for purposes that pursue a criminal law enforcement objective because the different purposes can very well be incompatible with each other even though the purposes pursue a similar LED objective.[543] Sometimes the compatibility test can be stopped after step one because the compatibility between purposes for the data collection and further use qualifies as, what I like to call, a *no-brainer*. This is particularly the case when personal data is not combined with other data and is further processed for the same purpose as for which the data was initially collected.[544] For example, a name and phone number is collected to register access for an individual to Service A of Company X. The phone number and name is further processed when the access is granted to the service two weeks later. In these cases the data controller is not obligated to assess the other aspects of the data processing and the mechanisms to mitigate the potential negative effects.

In other cases the compatibility between initial and new purposes is not as apparent and calls for the execution of the full assessment. In these cases the new purposes can, for example, slightly vary from the initial purposes, but because of the combination of data from multiple datasets the effects of the data processing differ and should be taken into account in the compatibility assessment. Company X from the previous example offers another service, Service B. To register to Service B a name, phone number and email address must be provided. On Service B company X wants to enforce a *real name policy*. When the company detects uncertainty with regard to the authenticity of the registered name, the access to Service B is blocked. The company combines the user databases of Service A and Service B and correlates the identities based on telephone numbers. In the cases where there are different names associated with the same telephone number, the company sends an email to the email address that is registered for Service B. In the email the company asks the data subject to provide a copy of her passport in order to verify the real name and unblock access to service B. The name that was provided for access to the services of company X is still processed for the purposes of access to the service but the effects of the real name policy enforcement for data subject are very different from the effects of registering for initial access.

The compatibility test includes an assessment of the foreseeability of the processing for the new processing purposes: could the data subject reasonably expect the

[543] EDPS, *Opinion on the Data Protection Reform Package*, 12 March 2012, par. 334.
[544] [Forgó et al., 2017].

further use of the data and what will be the consequences of the processing? The context of the data processing is an important factor too. This factor includes the characteristics of the context of the processing for the initial purposes, the question whether the data is switched from context, as well as the characteristics of the context of processing for the new purposes. The test must also take into account the possible consequences of the data processing and the nature of the data. It also includes looking at the measures that can be taken to mitigate the negative effects that might arise from the further processing. Without changing the new processing purposes circumstances, such as installing or deinstalling appropriate safeguards, influence the outcome of the compatibility test.

The compatibility test qualifies to a certain degree as a chicken-and-egg situation. The test is intended to investigate the compatibility between purposes, and with that, the proximity between the initial and new processing purposes.[545] Yet, the EDPB urges for a more thorough and comprehensive compatibility test when the purposes show a greater proximity.[546] This means that the outcome of the test dictates to a certain degree the method that has to be used to reach such an outcome. Circular reasonings like this are a common phenomenon in EU data protection law. Take, for example, the reasoning that is described on page 39: the substance of the fundamental right to protection of personal data is characterized by the substance of provisions from secondary data protection law. In turn, secondary data protection law aims for the protection of the fundamental right to protection of personal data.[547] Nonetheless, legal institutions manage to deal with these reasonings by viewing law as an interrelated set of rules and principles, where the parts must always be seen in the context of the whole. When individual rules of law are read out of context, the reader will soon discover that these rules of law are not necessarily based on the same rules of logic that underlie the computer programs that have to be compliant with those rules of law. The compatibility test should also be viewed through this lens: it consists of cumulative conditions that cannot be viewed separately, but have to be assessed based on their interrelationship, and thus on the whole of the circumstances of the case.

[545] [De Busser, 2009b, p. 168].

[546] Article 29 Working Party *Opinion on Purpose Limitation*, 2013, WP 203, p. 22.

[547] See to this extent the dissertation of Gloria Gonzales Fuster [Fuster, 2014b] and the work of Manon Oostveen that is based on her dissertation [Oostveen and Irion, 2018].

5.1.1.1 Precursors of the modern assessment

The DPD lacked guidelines for the compatibility assessment and Member States were highly divided on its substance. This was partly due to the broad wording of the purpose limitation principle, as acknowledged by the European Commission in the Evaluation of the DPD.[548] In 2002 Douwe Korff conducted a comparative study on the implementation of the DPD in the national laws of the EU Member States. The study aimed to inform the EU Commission and was meant to clarify whether there were differences in the way in which these implementations were applied. The results showed that the national implementations of the non-incompatibility requirement varied from an assessment of the reasonable expectations of the data subject (in certain cases in Belgium) to application of balancing tests (Germany and the Netherlands), or it was closely linked to the implementation and respect for other data protection principles, such as transparency, lawfulness and fairness (UK and Greece).[549] Up until the release of the *Opinion on Purpose Limitation* by the EDPB in 2013, there was no Union-wide interpretation of the compatibility assessment, the scope of derogations, and the need and type of safeguards for the rights and freedoms of the data subjects when personal data is further processed.[550]

The EDPB's *Opinion on Purpose Limitation* came at a strategic moment in time. The legislative process of the new regulatory framework was well underway and the European Commission had proposed to replace the non-incompatibility requirement with the requirement of allowing re-use when a new lawful processing ground could be obtained.[551] The EDPB's Opinion was inspired by the compatibility test in the Dutch implementation of the DPD.[552] This Dutch provision obligated the data controller to take into account the connection between the new and initial purposes, the nature of the data concerned, the effects of the processing on the data subject, the manner in which the data were collected, and the existence of appropriate safeguards.[553] In

[548] Evaluation of the Implementation of the DPD, par. 25 in Commission Staff Working Paper, Impact Assessment Accompanying the proposals for a Regulation and Directive, SEC(2012) 72 final, Annex 2.

[549] Douwe Korff, EC Study on Implementation of DPD Comparative Summary of national laws, Human Rights Centre, University of Essex, p. 63-66.

[550] Evaluation of the Implementation of the DPD, par. 25 in Commission Staff Working Paper, Impact Assessment Accompanying the proposals for a Regulation and Directive, SEC(2012) 72 final, Annex 2; Article 29 Working Party *Opinion on Purpose Limitation*, 2013, WP 203.

[551] This is discussed in Section 5.1.2.1 on 137 of this study.

[552] Article 9 Wet bescherming persoonsgegevens.

[553] See for an analysis of the criteria of art. 9 Wbp in relation to the GDPR and the Article 29 Working

the Opinion the EDPB made two important steps: firstly, they proposed guidelines on the compatibility test,[554] and, secondly, they proposed amendments to the GDPR that safeguarded the codification of these guidelines.[555] The final text of art. 6(4) GDPR differs from the proposed amendments but the general idea of a balancing compatibility test remained. The inclusion of this test is called by some law scholars "one of the real achievements of the GDPR".[556]

5.1.1.2 The compatibility factors of the modern assessment of art. 6(4) GDPR

In order to ascertain whether processing for a new purpose is compatible with the purpose for which the personal data are initially collected, the controller has to, pursuant to art. 6(4) juncto Recital 50 GDPR, take into account the following factors: the link between the purposes, the context of data collection, the nature of the personal data, the possible consequences of processing, and the existence of safeguards.[557] The compatibility factors are non-exhaustive and none of them are independently decisive. The assessment is meant to balance the outcomes of the various factors. The test should be conducted on a case-by-case base.[558]

5.1.1.3 No guidance on compatibility test in LED

The LED also includes a non-incompatibility requirement.[559] This law lacks, however, codified guidelines that are similar to art. 6(4) or Recital 50 GDPR, and, due to the mandate of the EDPB under the Date Protection Directive, the *Opinion on Purpose Limitation* does not connect the conclusions on the non-incompatibility requirement to data processing in the field of criminal law enforcement and public security.[560]

Party Opinion on Purpose Limitation [Wiebe and Dietrich, 2017, p. 58-86].

[554] Article 29 Working Party *Opinion on Purpose Limitation*, 2013, WP 203, p. 21 and 40.

[555] Article 29 Working Party *Opinion on Purpose Limitation*, 2013, WP 203, p. 43-44.

[556] [Forgó et al., 2017, p. 35].

[557] See also Section 3.3.6 on page 71 where these factors are introduced.

[558] Article 29 Working Party *Opinion on Purpose Limitation*, 2013, WP 203, p. 21; Caution and earnestness is advised when conducting this assessment. Unlawful processing data for incompatible purposes under the GDPR is subject to administrative fines up to 20 million Euro or 4 percent of the total worldwide annual turnover of the preceding financial year, whichever is higher. Article 83(5)(a) GDPR.

[559] See Sections 2.2.2.2 on page 52.

[560] Article 29 LED; Before the LED only data transfers between competent authorities in different Member States were regulated by EU law. See Section 2.2.2.2 on page 52 on this topic. In May 2017 the EDPS received the task of supervising the lawfulness of personal data processing by Europol. Article 43 Europol

On top of that, the LED is adopted pursuant to Declaration no. 21 of the Treaty of Lisbon,[561] that called for specific data protection rules in the field of judicial co-operation in criminal matters and police cooperation, which includes criminal law enforcement and public security.[562] During the legislative process of the new regulatory framework, some Member States called for an autonomous meaning of the concept of non-incompatibility in the field of criminal law enforcement and public security.[563] However, their proposals are not adopted in the final text and the legislator removed a reference to the discretion of the Member States on the definition of compatibility.[564] It is yet to be determined in the case law of the CJEU what the discretion of the Member States is when it comes to the meaning of compatibility and how the requirement should be interpreted in data protection law on police matters. However, given the conclusions that I will draw in Section 5.5.4, the answer to this question looses practical importance and qualifies as purely academic.

5.1.2 A requirement under pressure

The non-incompatibility requirement is part of the data protection principles, which are one of the four cumulating touchstones that have to be secured in order for data

Regulation.

[561] Recital 10 LED.

[562] Declaration no. 21 of the Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community, signed at Lisbon, 13 December 2007 – Declaration on the protection of personal data in the fields of judicial cooperation in criminal matters and police cooperation. See for an in-depth study of the legal framework of data protection in the field of police cooperation prior to the changes following this declaration, and the new regulatory framework and the new Europol Regulation: [De Busser, 2009a].

[563] Commented and Revised 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 offenses or the execution of criminal penalties, and the free movement of such data, European Commission 29 June 2015, Note 10335/15, number of the Commission Document 5833/12, footnote 151 and 151, p. 50; See also [Jasserand, 2018, p. 158]. She argues that the Member States have a margin of discretion in the definition of non-incompatibility.

[564] See the previous framework: Framework Decision 2008/977/JHA, which was discussed in Section 2.2.2.2 on page 52. This stated that that "Framework Decision should leave it to Member States to determine more precisely at national level which other purposes are to be considered as incompatible with the purpose for which the personal data were originally collected." Recital 6 Council Framework Decision 2008/977/JHA,On The Protection Of Personal Data Processed In The Framework Of Police And Judicial Cooperation In Criminal Matters.

processing to be legitimate under the European data protection framework.[565] However, the value and systematic application of the requirement is not as straightforward as with the other data protection principles. The European Commission attenuated the requirement in its first draft of the GDPR by proposing that whenever further processing is incompatible with the initial purposes, the processing must have a legal basis in at least one of the lawful processing grounds.[566]

If this provision had been adopted re-use of data would have been made quite easy, easy to the extent that the non-incompatibility requirement would have lost its protective value in the limitation of data use. Also the CJEU has ruled on cases that concerned further use of data, but never has it conducted a compatibility assessment of initial and new processing purposes, let alone, relied on the factors of the modern assessment in its reasoning.[567] The following sections describe what the arguments were in the Commission proposal and detail the CJEU reasonings.

5.1.2.1 Watered-down purpose limitation in the EU Commission's draft of the GDPR

In the 2012 European Commission's proposal of the GDPR (dGDPR) the general idea of cumulation of touchstones was abandoned with regard to the non-incompatibility requirement.[568] The Commission proposed the possibility for the data controller to evade this requirement by starting to process readily collected personal data for new and incompatible processing purposes on the base of new processing grounds.[569]

The text of the draft article 6(4) dGDPR was:

> Where the purpose of further processing is not compatible with the one for which the personal data have been collected, the processing must have a legal basis at least in one of the grounds referred to in points (a) to (e) of paragraph 1. This shall in particular apply to any change of terms and general conditions of a contract.

[565] See Section 3.5 on 79.

[566] See Section 5.1.2.1 in this topic.

[567] See Section 5.1.2.2 on this topic.

[568] See Section 3.5 on page 79 for the four comprehensive touchstones of data protection; dGDPR COM(2012) 11 final Proposal for a Regulation 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).

[569] See Section 3.5.2 on page 83 of this study for a discussion of this processing grounds.

This would circumvent the carefully drafted system of derogations that is based on the free will of the data subject who has provided renewed consent or is grounded in a *lex specialis* that is based on a system of safeguards that protect against fundamental rights violations.[570] Article 6(4) dGDPR did not include such safeguards.[571] On top of this, the European Council included in a later version of the draft the f-ground in art. 6(4) dGDPR, which meant that personal data that was initially processed on the base of, for example, consent could be re-used for new purposes on the base of the legitimate interests of the data controller without the data subject being included in this decision making process.[572] Privacy advocates were up in arms and – amongst other things – 66 non-governmental organizations expressed their concerns in a letter to the European Commission President.[573] The organizations argued that with this proposal the Council had dropped below the levels of protection provided by the DPD, which would have been contrary to the earlier promises made by the European Commission.

The EU Parliament showed staunch opposition against these proposals and discarded the passage of the Commission and that of the Council.[574] Instead the Parliament included the factors of the non-compatibility test the final text of art. 6(4) GDPR, which were discussed in Section 3.3.6 on page 71 and Section 5.1.1 on page 131 and specified only two processing grounds on which re-use can be based, renewed consent[575] and a *lex specialis* that targets the objectives listed in art. 23(1) GDPR and safeguards against fundamental rights violations.[576]

[570] See Section 5.2 and Section 5.3.

[571] See, for example the position paper of the European Digital rights Initiative (Edri), that warned about the dangers of circumventing derogation clauses with the proposed art. 6(4) Draft GDPR; *Key aspects of the proposed General Data Protection Regulation explained: What are they? Why are they important? What are common misconceptions? What can be improved?*, Edri, 26 November 2012, p. 3. Available on https://edri.org/files/GDPR-key-issues-explained.pdf Lastly retrieved 22 December 2019.

[572] https://edri.org/files/EP_Council_Comparison.pdf Lastly retrieved 22 December 2019; European Council on June 15, 2015, 9565/15.

[573] https://edri.org/files/DP_letter_Juncker_20150421.pdf. Lastly retrieved 22 December 2019.

[574] 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) (COM(2012)0011-C7-0025/2012-2012/0011(COD)), T7-0212/2014. Available on http://www.europarl.europa.eu/sides/getDoc.do?type=TA&language=EN&reference=P7-TA-2014-0212 Lastly retrieved 22 December 2019.

[575] See Section 5.3.

[576] See Section 5.2 to this extent.

5.1.2.2 Systematic omission of the non-incompatibility requirement by the CJEU in the appraisal of an interference with and its impact on the rights of art. 7 and 8 CFREU

From the case law investigated for this study the following conclusion can be drawn: In the assessment of the establishment of an interference with and the impact on the rights protected under the Charter the CJEU has never taken into account the role of the non-incompatibility requirement. The following section discusses the relevant case law and analyzes on what aspects the CJEU did focus.

5.1.2.2.1 The *Schwarz*- and *Willems*-case: Legalism instead of the non-incompatibility requirement The *Schwarz*-case concerned the processing of biometric data for the purposes of passport validation and the verification of the identity of the passport holder.[577] The CJEU explained that the purposes were stipulated in Regulation 2252/2004/EC (Passport Regulation) and that the processing should be considered a justifiable restriction on the rights protected in art. 7 and 8 CFREU.[578] The interference was partly legitimized by the strict purpose specification of the Passport Regulation.[579]

The *Willems*-case concerned the further use of the data that was initially collected for the purposes of the passport Regulation.[580] The referring national court asked the CJEU in preliminary questions whether art. 4(3) of the Passport Regulation in light of art. 7 and 8 of the CFREU, art. 8(2) of the ECHR and art. 6(1)(f) GDPR, read in conjunction with the purpose limitation principle as laid down in art. 5(1)(b) GDPR, require a guarantee that when collecting biometric data under the Passport Regulation, Member States have to comply with the requirement of non-incompatibility, in a sense that the biometric data could only be processed for the original or compatible purposes for which the data was collected.[581] To answer this question, the CJEU

[577] CJEU 10 October 2013, C-291/12, (*Michael Schwarz/Stadt Bochum*).

[578] CJEU 10 October 2013, C-291/12, (*Michael Schwarz/Stadt Bochum*), par. 64-66.

[579] CJEU 10 October 2013, C-291/12, (*Michael Schwarz/Stadt Bochum*), par. 60-63.

[580] CJEU 16 April 2015, C-446/12, C-447/12, C-448/12, C-449/12, (*W. P. Willems/Burgemeester van Nuth, H. J. Kooistra/Burgemeester van Skarsterlân, M. Roest/Burgemeester van Amsterdam, L. J. A. van Luijk/Burgemeester van Den Haag*).

[581] CJEU 16 April 2015, C-446/12, C-447/12, C-448/12, C-449/12, (*W. P. Willems/Burgemeester van Nuth, H. J. Kooistra/Burgemeester van Skarsterlân, M. Roest/Burgemeester van Amsterdam, L. J. A. van Luijk/Burgemeester van Den Haag*), par. 29.

referred to the *Åkerberg Fransson*-case and *Texdata Software*-case that were discussed on page 34.[582] These cases underline that the CFREU follows EU law. The CJEU explained that since the Passport Regulation is not applicable to the processing of data for other purposes than the ones that are narrowly formulated in the purpose specification of that specific regulation, the Charter is also not applicable to the processing for those other purposes since that processing is not rooted in EU law.[583]

The CJEU did not investigate if other rules derived from EU law – most glaringly the non-incompatibility requirement ex art. 5(1)(b) GDPR – might apply to the further use of the data that was collected under the passport Regulation.[584] Analogous reasoning would result in the following rule: Further processing for new purposes of personal data that was initially collected for purposes stemming from EU law, is positioned outside the scope of EU law when the further processing operation is not instructed by the EU legislature. Did the CJEU just drop a bomb on the requirement of non-incompatibility or was this a slip of the pen?

The *Willems*-case is heavily criticized by legal scholars, who accuse the CJEU of following an inappropriate and dangerous form of legalism.[585] The main critique resides in the exclusion of the GDPR in the answers of the CJEU. And I agree. In my opinion the CJEU had to include the GDPR in answering the questions, in particular

[582] CJEU 16 April 2015, C-446/12, C-447/12, C-448/12, C-449/12, (*W. P. Willems/Burgemeester van Nuth, H. J. Kooistra/Burgemeester van Skarsterlân, M. Roest/Burgemeester van Amsterdam, L. J. A. van Luijk/Burgemeester van Den Haag*), par. 49; CJEU 26 February 2013, C-617/10, (*Åklagaren/Hans Åkerberg Fransson*), par. 20-22; CJEU 26 September 2013, C-418/11 (*Texdata Software*), par. 71-73.

[583] CJEU 16 April 2015, C-446/12, C-447/12, C-448/12, C-449/12, (*W. P. Willems/Burgemeester van Nuth, H. J. Kooistra/Burgemeester van Skarsterlân, M. Roest/Burgemeester van Amsterdam, L. J. A. van Luijk/Burgemeester van Den Haag*), par. 45, 47, 49-50.

[584] Article 5(1)(b) GDPR was even included in the question. If the question was unclear to the CJEU it also showed no interest in rephrasing the preliminary questions. In other data protection cases the CJEU did not hold back and conducted some serious rephrasing before answering the relevant questions that surrounded the matter at stake. See for example the *Bara*-case that is discussed in Section 5.1.2.2.3. CJEU 1 October 2015, C-201/14 (*Smaranda Bara and Others*).

[585] See for example: Eduardo Gill-Pedro, 'Joined Cases C-446/12 - 449/12 Willems: The CJEU washes its hands of Member States' fingerprint retention', European Law Blog, April 29 2015, available on: http://europeanlawblog.eu/2015/04/29/joined-cases-c-44612-44912-willems-the-cjeu-washes-its-hands-of-member-states-fingerprint-retention/. Lastly retrieved 22 December 2019; Steve Peers, ' Biometric data and data protection law: the CJEU loses the plot', EU Law Analysis, April 17 2015, available on: http://eulawanalysis.blogspot.nl/2015/04/biometric-data-and-data-protection-law.html Lastly retrieved 22 December 2019.

the non-incompatibility requirement ex art. 5(1)(b) GDPR. It would have been in-line with the legislative developments at the time, if the CJEU would have advised the national Court to assess the compatibility between the purposes of further processing with the initial purposes of collecting the data pursuant to the passport Regulation.[586]

Anticipating on a conclusion of non-compatibility, the CJEU could have taken the same line of reasoning that it demonstrated in the *Tele2*-case a year later.[587] That case offers a framework to assess data processing that restricts the data protection principles when it interferes with the rights protected under art. 7 and 8 CFREU. The *Tele2*-case concerned the function of art. 15 e-Privacy Directive, the restriction clause of the e-Privacy Directive. The function of that provision is similar to the function of a *lex specialis* derogation ex art. 6(4) juncto 23(1) GDPR, which will de discussed in Section 5.2. The conclusion from the *Tele2*-judgement can, therefore, be partly copied to the system of protection offered by the GDPR.

In that light, the most important conclusion from the *Tele2*-case concerns the structure of EU laws. The CJEU explained that legislative measures that are taken pursuant to art. 15(1) ePrivacy Directive are not excluded from the scope of that directive, for otherwise that provision would be deprived of any purpose. An exemption clause, such as art. 15 ePrivacy Directive and the derogations of art. 6(4) GDPR, necessarily presupposes that the national measures referred to therein fall within the scope of EU law, since it expressly authorizes the Member States to adopt them only if the conditions that have been laid down in the restriction or derogation clauses are met. So, if in the *Willems*-case the further processing of personal data for new purposes is incompatible with the initial purposes from the Passport Regulation, the only lawful option for re-use would be on the base of a measure that meets the conditions of art. 6(4) juncto 23(1) GDPR. The national measure that administers such re-use falls under the scope of EU law.[588]

5.1.2.2.2 The *Digital Rights Ireland*- and *Tele2*-case: transparency, data minimization, storage limitation and confidentiality instead of the non-incompatibility requirement The *Digital Rights Ireland* and *Tele2*-case concerned telecommu-

[586] The Opinion of the EDPB on Purpose Limitation of 2013 could have guided the CJEU in explaining how to make this assessment.

[587] See the next section.

[588] CJEU 21 December 2016, C-203/15 and C-698/15 (*Tele2 Sverige/Post- och telestyrelsen* and *Secretary of State for the Home Department/Tom Watson, Peter Brice, Geoffrey Lewis*), par 73.

nication metadata that was initially processed for commercial purposes by telecommunication providers and continued to be processed for the purposes of keeping the data available for competent authorities in their task of prevention, investigation, detection or prosecution of criminal offenses.[589] The *Tele2*-case builds on the *Digital Rights Ireland*-case and both cases concern re-use of personal data.[590] However, while assessing the existence and the impact of the interference, the CJEU was silent on the non-incompatibility requirement. Rather, the CJEU based its reasoning on other data protection principles which it implicitly weaved through its considerations.

The transparency principle ex art. 5(1)(a) GDPR lays the base when the CJEU considered that the interference was particularly serious because the "data are retained and subsequently used without the subscriber or registered user being informed" and this aspect is considered by the Court to likely "generate in the minds of the persons concerned the feeling that their private lives are the subject of constant surveillance."[591] The data minimization and storage limitation principles ex art. 5(1)(c) and (e) GDPR lay the groundwork for the retention arguments. The CJEU underlined that the measures imposed on the providers of publicly available electronic communications services or on public communications networks obligate to retain systematically and continuously, with no exceptions, data relating to a person's private life and to her communications.[592] The CJEU explained that this, regardless of the storage being for a certain period, constitutes in itself an interference with the rights guaranteed by

[589] CJEU 8 April 2014, joined cases C-293/12, C-594/12, (*Digital Rights Ireland Ltd/Ireland, and Kärntner Landesregierung/Michael Seitlinger, Christof Tschohl and others*); CJEU 21 December 2016, C-203/15 and C-698/15 (*Tele2 Sverige/Post- och telestyrelsen* and *Secretary of State for the Home Department/Tom Watson, Peter Brice, Geoffrey Lewis*).

[590] See European Human Right Cases 2017/79, M.E. Koning, *Annotation to CJEU Tele2, C 203/15 and C-698/15*; and European Human Right Cases 2014/140, M.E. Koning, *Annotation to CJEU Digital Rights Ireland, C-293/12 and C-594/12*; See also [Guild and Carrera, 2014] that looks at the aftermath of the Digital Right Ireland-case in the EU and [Kosta, 2013b] on the national court rulings on metadata retention and the Data Retention Directive.

[591] CJEU 8 April 2014, joined cases C-293/12, C-594/12, (*Digital Rights Ireland Ltd/Ireland, and Kärntner Landesregierung/Michael Seitlinger, Christof Tschohl and others*), par. 37; CJEU 21 December 2016, C-203/15 and C-698/15 (*Tele2 Sverige/Post- och telestyrelsen* and *Secretary of State for the Home Department/Tom Watson, Peter Brice, Geoffrey Lewis*), par. 100.

[592] CJEU 8 April 2014, joined cases C-293/12, C-594/12, (*Digital Rights Ireland Ltd/Ireland, and Kärntner Landesregierung/Michael Seitlinger, Christof Tschohl and others*), par. 34; CJEU 21 December 2016, C-203/15 and C-698/15 (*Tele2 Sverige/Post- och telestyrelsen* and *Secretary of State for the Home Department/Tom Watson, Peter Brice, Geoffrey Lewis*), par. 97.

art. 7 CFREU.[593] The confidentiality of the data was also considered to be at stake, because the competent authorities could gain access to the retained data, which taken as a whole, was liable to allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained.[594]

Despite the fact that the disputed data retention measures permitted re-use, the CJEU did not connect the derogation from the non-incompatibility requirement to the existence of the interference and the impact of the interference in either case.

5.1.2.2.3 The *Bara*-case: Lawfulness, fairness and transparency instead of the non-incompatibility requirement The *Bara*-case brought a similar opportunity for the CJEU to rule on the non-incompatibility requirement, yet again it chose to ignore this. The applicants in the *Bara*-case brought an appeal before the Romanian Court of Appeal, in which they challenged the lawfulness of a transfer of tax data relating to their income.[595] Their personal data was, on the basis of an internal protocol, transferred and used for purposes other than those for which it had initially been collected, without their prior explicit consent and without them being informed.[596] The questions referred by the national Court of Appeal were – in all honesty – not free from ambiguity and could have benefited from more precise expression.[597] Three out of four questions were declared inadmissible,[598] and the fourth question was rephrased by the CJEU.

The initial question was:

> May personal data be processed by authorities for which such data were

[593] CJEU 8 April 2014, joined cases C-293/12, C-594/12, (*Digital Rights Ireland Ltd/Ireland, and Kärntner Landesregierung/Michael Seitlinger, Christof Tschohl and others*), par. 34; CJEU 21 December 2016, C-203/15 and C-698/15 (*Tele2 Sverige/Post- och telestyrelsen* and *Secretary of State for the Home Department/Tom Watson, Peter Brice, Geoffrey Lewis*), par. 97.

[594] The CJEU lists the following examples: such as everyday habits, permanent or temporary places of residence, daily or other movements, the activities carried out, the social relationships of those persons and the social environments frequented by them. CJEU 8 April 2014, joined cases C-293/12, C-594/12, (*Digital Rights Ireland Ltd/Ireland, and Kärntner Landesregierung/Michael Seitlinger, Christof Tschohl and others*), par. 27 and 35; CJEU 21 December 2016, C-203/15 and C-698/15 (*Tele2 Sverige/Post- och telestyrelsen* and *Secretary of State for the Home Department/Tom Watson, Peter Brice, Geoffrey Lewis*), par. 88 and 99.

[595] CJEU 1 October 2015, C-201/14 (*Smaranda Bara and Others*).

[596] CJEU 1 October 2015, C-201/14 (*Smaranda Bara and Others*), par. 15.

[597] See the work of Bobek, who investigated the dialogue between eastern European Member States and the CJEU in preliminary references: [Bobek, 2008].

[598] CJEU 1 October 2015, C-201/14 (*Smaranda Bara and Others*), par. 19-24.

> not intended where such an operation gives rise, retroactively, to financial loss?[599]

In my view the referring court asked:

> Can personal data be processed for new and potentially incompatible purposes when such processing operations lead to financial loss with the data subjects?

This would have pointed the CJEU in the direction of art. 5(1)(b) GDPR, the 2013 Opinion on Purpose Limitation from the EDPB[600] and art. 6(4) and art. 23 GDPR. Instead, the CJEU rephrased the preliminary question to:

> Must articles 13, 14 and 23 of the GDPR be interpreted as precluding national measures, such as those at issue in the main proceedings, which allow a public administrative body in a Member State to transfer personal data to another public administrative body and their subsequent processing, without the data subjects being informed of that transfer and processing?[601]

The CJEU shifts the focus to the principles of lawfulness, fairness and transparency ex art. 5(1)(a) GDPR and the requirement of non-incompatibility ex art. 5(1)(b) GDPR is excluded from the CJEU's interpretation of the legal issues at stake.

The sections above have revealed that the CJEU is not particularly keen on including the requirement of non-incompatibility when it comes to the acknowledgement of an interference with and its impact on the rights and freedoms of the data subject.

[599] CJEU 1 October 2015, C-201/14 (*Smaranda Bara and Others*), par. 18.

[600] See Section 5.1.1.1.

[601] Original text: "By its fourth question, the referring court asks, in essence, whether Articles 10, 11 and 13 of Directive 95/46 must be interpreted as precluding national measures, such as those at issue in the main proceedings, which allow a public administrative body in a Member State to transfer personal data to another public administrative body and their subsequent processing, without the data subjects being informed of that transfer and processing." CJEU 1 October 2015, C-201/14 (*Smaranda Bara and Others*), par. 28.

5.1.3 The ingraining of the compatibility factors in the art. 8(1) ECHR assessments of the ECtHR

The legal EU framework on further use does not exist in a vacuum. Section 2.1.1.1 described that, in cases that concerned further use of data for new purposes, the reasonable expectations of the person to whom the data related are taken into account by the ECtHR in its assessment of the existence and impact of an interference with the rights protected under art. 8(1) ECHR. This section discusses in more detail how this and other factors of the compatibility test can be found in the appraisal of art. 8(1) ECHR by the ECtHR. The following subquestions are partly answered in the following sections: "To what extent does further use of personal data lead to an infringement of fundamental rights?" and "To what extent do limitations on the non-incompatibility requirement lead to an infringement of fundamental rights?".

5.1.3.1 Link between the purposes

For the further processing of data that would fall under the scope of the GDPR in EU law, the ECtHR has evaluated the existence of an infringement of the right to respect for private life by investigating the foreseeability of the further use.[602] In doing so, the ECtHR indirectly investigated the proximity between the purposes and compared the initial purpose of processing to the new processing purposes. Take, for example, the *M.S./Sweden*-case, which concerned the disclosure of medical files with information about an abortion by a governmental medical clinic to another public authority.[603] The applicant's information had been collected and stored at the clinic in connection with a medical treatment, but was subsequently communicated for a different purpose, namely, to enable the Social Insurance Office to examine the applicant's claim for compensation under the Industrial Injury Insurance Act.[604] The ECtHR explained that it did not follow from the fact that the applicant had sought treatment at the

[602] ECtHR 25 September 2001, no.44787/98 (*P.G. and J.H./the United Kingdom*), par. 57; ECtHR 7 July 2003, no. 63737/00 (*Perry/the United Kingdom*), par. 38; ECtHR 2 September 2010, no. 35623/05 (*Uzun/Turkey*), par. 44; ECtHR 18 October 2016, no. 61838/10 (*Vukota-Bojić v. Switzerland*), par. 55; ECtHR 23 February 2016, no. 40378/06 (*Y.Y./Russia*).

[603] ECtHR 27 August 1997, no. 20837/92 (*M.S./Sweden*)

[604] ECtHR 27 August 1997, no. 20837/92 (*M.S./Sweden*), par. 10.

clinic that she would consent to the data being disclosed to the Office.[605] The Court found that the disclosure of the data by the clinic to the Office entailed an interference with the applicant's right to respect for private life as guaranteed by art. 8(1) ECHR.[606]

A similar approach was used in the *Peck*-case.[607] In this case the ECtHR took into account the foreseeability and also the context of processing, which will be separately discussed in Section 5.1.3.2. The case concerned CCTV footage of a suicide attempt that was shared by the police with the media. Here, data was initially collected for criminal law enforcement purposes by the police that would fall under the scope of the LED in the EU and it was further processed by the media for purposes that would fall under the scope of the GDPR. In the ruling the initial and new processing purposes were compared and the foreseeability of the further processing of the data was taken into account. The ECtHR regarded the initial data collection by means of the CCTV camera not invasive to privacy, but the subsequent data processing was regarded as such.[608] Because the data was shared with the media, the suicide attempt was viewed to an extent which far exceeded any exposure to a passer-by or security observation.[609] This exposure surpassed the degree of exposure which the applicant could possibly have foreseen when he walked outside on the streets. The ECtHR concluded that the disclosure by the authorities of the data constituted a serious interference with the applicant's right to respect for his private life.[610]

These cases illustrate that the ECtHR investigates the link of and proximity between initial and new purposes through the criteria of foreseeability in cases that concern the processing of personal data for new purposes that would fall under the GDPR and when LED-data is further used for GDPR purposes.

5.1.3.2 The context of processing

As described on page 133 the factor *context* includes the characteristics of the context of the processing for the initial purposes, the characteristics of the context of process-

[605] See in this regard [Evers, 2016], who mapped the factor of foreseeability in disclossing of medical data.

[606] ECtHR 27 August 1997, no. 20837/92 (*M.S./Sweden*), par. 35.

[607] ECtHR 28 January 2003, no. 44647/98 (*Peck/the United Kingdom*).

[608] ECtHR 28 January 2003, no. 44647/98 (*Peck/the United Kingdom*), par. 58-59.

[609] ECtHR 28 January 2003, no. 44647/98 (*Peck/the United Kingdom*), par. 62.

[610] ECtHR 28 January 2003, no. 44647/98 (*Peck/the United Kingdom*), par. 62-63.

ing for the new purposes, as well as the question whether the data is switched from context. In the case law of the ECtHR regarding the assessment of an interference with the rights protected under art. 8(1) ECHR, the context is taken into account of the data collection, the further processing and their relation.

The most noticeable examples of how the initial context of the data collection is considered in the appreciation of the rights protected under art. 8(1) ECHR, can be found in cases in which the mere data collection is enough to amount to an interference. This can be seen in cases that concerned data collection in the context of criminal law enforcement and public security.[611] In those cases, which will be discussed in Section 5.5.2 of this study, the context of the data collection for the initial processing purposes was decisive, and not the actual further use of data.

In the *Peck*-case, which was discussed in Section 5.1.3.1 of this study, data that was collected in a police context entered the commercial media context.[612] The ECtHR also ruled on cases where data switched context the other way around, from being collected for commercial purposes that would fall under the GDPR in EU law, to further use in a police context for purposes that would fall under the scope of the LED in EU law. The *Malone*- and *P.G. and J.H.*-cases make good examples of this, because those concered telecommunication metadata collection by the police from telecommunication providers.[613] In these judgements the ECtHR explained that the processing of metadata does not interfere *per se* with the rights of art. 8(1) ECHR, when this, for example, happens for billing purposes by the telecommunication providers. However, the ECtHR underlines that when this data is obtained by the police and switches context, private life concerns do arise.[614]

The case law discussion shows that the context of processing is part of the ECtHR's reasoning while asserting the interference with the rights protected under art. 8(1) ECHR in cases that concern the further use of data relating to private life.

---

[611] See for example ECtHR 17 December 2009, no. 16428/05 (*Gardel/France*), par. 58; ECtHR 26 January 1999, no. 42293/98 (*Adamson/the United Kingdom*).

[612] ECtHR 28 January 2003, no. 44647/98 (*Peck/the United Kingdom*).

[613] ECtHR 25 September 2001, no.44787/98 (*P.G. and J.H./the United Kingdom*); ECtHR 2 August 1984, no. 8691/79 (*Malone/the United Kingdom*).

[614] ECtHR 25 September 2001, no.44787/98 (*P.G. and J.H./the United Kingdom*) par. 42; ECtHR 2 August 1984, no. 8691/79 (*Malone/the United Kingdom*), par. 84.

5.1.3.3 The nature of the personal data

On multiple occasions the ECtHR took into account the nature of the data while assessing the further use of data relating to private life. The ECtHR only needed a few words to connect, for example, the further use of information to the nature of the data in a sex offenders registry, which combined identifying information, data on criminal matters and potentially psychological and sexual health information.[615] In the *Gardel*-case, for instance, the ECtHR stressed that it is not its task to speculate on the sensitive nature of the information gathered or on the possible difficulties experienced by the applicant who was registered as a sex offender because the requirement for persons convicted of sexual offenses to inform the police of their name, date of birth, address or change of address falls in itself within the scope of art. 8(1) ECHR.[616]

There is also long list of case law where disclosures of medical data for new purposes to third parties lead to an infringement with the right protected under art. 8(1) ECHR.[617] In these cases the nature of the data played a trivial role in the ECtHR's assessment.

For example, the *Y.Y. v. Russia*-case that was brought before the ECtHR after an investigation by a government Committee for Healthcare into the cause of death of one of two twins at birth.[618] The investigation was requested by a third person, the grandmother of the twins, who maintained a disruptive relationship with her daughter. The Committee for Healthcare collected all medical information about the twins and their mother from the maternity hospital. Based on the provided information the Committee concluded that no abnormalities had occurred surrounding the birth of the twins. The Committee's report was then shared with the Ministry of Health, the mother and the third person. The report contained information about the delivery, but also the number of previous pregnancies that had not resulted in deliveries. At no stage of the investigation the mother's consent was sought or received. Stunned by the existence of the investigation the mother launched a complaint against the Committee for collecting the information at the maternity hospital and sharing the report

[615] See for example ECtHR 26 January 1999, no. 42293/98 (*Adamson/the United Kingdom*).

[616] ECtHR 17 December 2009, no. 16428/05 (*Gardel/France*), par. 58.

[617] See for example ECtHR 6 June 2013, no. 1585/09 (*Avilkina/Russia*), par. 32; ECtHR 15 April 2014, no. 50073/07 (*Radu v. the Republic of Moldova*), par. 27; ECtHR 29 April 2014, no. 52019/07 (*L.H./Latvia*), par. 33.

[618] ECtHR 23 February 2016, no. 40378/06 (*Y.Y./Russia*).

with the Ministry of Health and the third person without her knowledge and consent. The ECtHR underlined that the information in the report was of particularly private and sensitive nature and that it followed that the dissemination of it for new purposes without the consent of the mother constituted an interference with the right to respect for private life, ex art. 8(1) ECHR.[619] The nature of the data is factored in the reasonings of the ECtHR in cases that concern further use of data for new purposes.

5.1.3.4 Possible consequences

The possible consequences of further data processing are taken into account by the ECtHR when acknowledging an interference with the right to respect for private life. The *P.G. and J.H.*-case, for example, concerned government records that contained personal data.[620] Those records were subjected to a process of analysis directly relevant to identifying the person in the context of other personal data. Regardless of the data being recorded in a more public space, the ECtHR considered the processing an interference with the right to respect for private life within the meaning of art. 8(1) ECHR because of the further processing and its consequences.[621]

The ECtHR accepts that complaints about data storage oftentimes do not arise from the retention itself but from the fact that, if stored, disclosure or further processing may follow.[622] In the *S. and Marper*-case, for example, the ECtHR took into account the rapid pace of developments in the field of genetics and information technology and explained that it cannot discount the possibility that in the future the private-life interests that relate with genetic information may be adversely affected in novel ways or in a manner which cannot be anticipated with precision today.[623] Similar reasoning can be found in the *van der Velden*-case in which the Commission considered that, given the use to which it could conceivably be put in the future, the systematic retention of cellular material goes beyond the scope of neutral identifying features, and is, therefore, sufficiently intrusive to constitute an interference with the right set out in Article 8(1) of the Convention.[624]

[619] ECtHR 23 February 2016, no. 40378/06 (*Y.Y./Russia*),par. 40-42.
[620] ECtHR 25 September 2001, no.44787/98 (*P.G. and J.H./the United Kingdom*).
[621] ECtHR 25 September 2001, no.44787/98 (*P.G. and J.H./the United Kingdom*) par. 59.
[622] See for example ECtHR 13 November 2012, no. 24029/07 (*M.M./the United Kingdom*), par. 159.
[623] ECtHR 4 December 2008, no.130562/04 and 30566/04 (*S. and Marper/the United Kingdom*), par. 72.
[624] EComHR 7 December 2006, no. 29514/05, (*van der Velden/the Netherlands*).

Potential future violations gain prominence when some of the information that is stored or disseminated has been declared false and is likely to injure the applicant's reputation.[625] In the *Cemalettin Canli*-case, for example, a police file was disseminated in which the applicant was not referred to as someone who had been *accused of*, *charged with* or *prosecuted for* the offense of membership of an illegal organization, but as being a *member* of such an organization. The ECtHR considered that referring to the applicant as a *member* was potentially damaging to his reputation because the applicant has never been convicted by a court of law in relation to this offense. The ECtHR explained that art. 8(1) of the Convention was applicable and that the continued storage and dissemination of the data constituted an interference with the applicant's right to respect for his private life.[626]

The possible consequences of the further processing of data are scrutinized by the ECtHR in its assessment of the interference with the rights protected under art. 8(1) ECHR and the impact thereof.

5.1.3.5 Safeguards

In a few cases the ECtHR demonstrated that safeguards come into play when regarding the establishment of an interference of and its impact on the rights protected in art. 8(1) ECHR. Take, for example, the *Leander*-case in which the further use of data from a secret police register was contested.[627] The ECtHR considered that the storing and the release of the information in light of the refusal to allow the applicant an opportunity to refute it, amounted to an interference with the right to respect for private life as guaranteed by art. 8(1) ECHR.[628] Similar deliberations can be found in the In the *M.M./the United Kingdom*-case, in which the ECtHR underlined that when a data subject is able to have her data deleted or some other remedy that would prevent dissemination, the data would no longer be available for disclosure and future interference.[629] Therefore, any examination of safeguards and available remedies must necessarily encompass alleged past, present and potential future violations in respect of the retention and disclosure of data.[630] Though the role of the assessments of the

[625] ECtHR 4 May 2000, no. 28341/95 (*Rotaru/Romania*), par. 44
[626] ECtHR 18 November 2008, no. 22427/04 (*Cemalettin Canli/Turkey*) par. 35-37.
[627] ECtHR 26 March 1987, no. 9248/81, (*Leander/Sweden*).
[628] ECtHR 26 March 1987, no. 9248/81, (*Leander/Sweden*), par. 48.
[629] ECtHR 13 November 2012, no. 24029/07 (*M.M./the United Kingdom*), par. 159.
[630] ECtHR 13 November 2012, no. 24029/07 (*M.M./the United Kingdom*), par. 159.

safeguards is small in this stage of the art. 8 ECHR considerations, they are taken into account in the art. 8(1) ECHR assessment in some cases by the ECtHR.

5.1.4 Conclusion on the non-incompatibility requirement

The requirement of non-incompatibility is part of European data protection law since the early Eighties, yet there was no common understanding as to how to assess the compatibility between purposes. As described at page 134 the EDPB introduced a test that balanced multiple factors, which has been adopted as positive law by means of art. 6(4) GDPR. It is unclear from the data protection framework and explanations that accompanied the legislative track of the new regulatory framework whether the assessment based on the balancing factors can be applied to the assessment of further use in the field of criminal law enforcement and public security too. However, as will be discussed in the upcoming sections this question is not as relevant as it might appear. All factors of the compatibility test have been taken into account individually or in conjunction with each other by the ECtHR in the assessment of infringements of and their impact on art. 8(1) ECHR in cases that concerned the further use of data. This case law can be used to substantiate the different factors of the compatibility assessment.

5.2 Re-use based on a *lex specialis* as required in art. 6(4) GDPR

The following section discusses the legitimate derogation that can be made on the non-incompatibility requirement with a *lex specialis* that is based on art. 6(4) juncto 23(1) GDPR. This section focusses on the answer to the research subquestion: What other types of limitations on data processing are implemented in European data protection law? This section also investigates the relationship between the purpose limitation principle and this other type of use limitation and in what way the non-incompatibility requirement is connected to the justification criteria for fundamental rights infringements.

5.2.1 The exclusion of the non-incompatibility requirement from the scope of art. 23 GDPR

Article 23 GDPR sets forward the criteria to restrict the scope of the obligations and rights provided for in art. 34 and art. 12 to 22 GDPR and the corresponding aspects of the storage limitation-, data minimization-, transparency- and accuracy principle ex art. 5(1) GDPR. The restrictions must respect the essence of fundamental rights and freedoms, be necessary and proportionate, and must pursue of a legitimate aim as exhaustively listed in art. 23(1)(a) to (j) GDPR.[631] In accordance with art. 23(2) GDPR the restriction must be laid down in a legislative measure that specifies:

- the purposes of the processing;
- the categories of personal data;
- the scope of the restrictions;
- the safeguards to prevent abuse or unlawful access or transfer;
- the controller or categories of controllers;
- the retention periods and the applicable safeguards taking into account the nature, scope and purposes of the processing or categories of processing;
- the risks to the rights and freedoms of data subjects; and
- the right of data subjects to be informed about the restriction, unless that may be prejudicial to the purpose of the restriction.

I believe it is a common misunderstanding that the non-incompatibility requirement is restrictable under art. 23(1) GDPR. Some scholars have carefully hinted at

[631] These aims are: national security; defence; public security; the prevention, investigation, detection or prosecution of criminal offenses or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security; other important objectives of general public interest of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, including monetary, budgetary and taxation a matters, public health and social security; the protection of judicial independence and judicial proceedings; the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions; a monitoring, inspection or regulatory function connected, even occasionally, to the exercise of official authority in the cases referred to in points (a) to (e) and (g) of art. 23 GDPR; the protection of the data subject or the rights and freedoms of others; and, the enforcement of civil law claims.

this position in the past, but ignored its implications by assuming that the EU legislature must have yielded the restriction of the non-incompatibility requirement under art. 23(1) GDPR *implicitly*.[632] I disagree and argue that the implicit or explicit restriction of the purpose limitation principle, consisting of the purpose specification requirement as well as the non-incompatibility requirement, is not made possible by art. 23(1) GDPR.

5.2.1.1 The restrictable data protection principles under art. 23(1) GDPR

Article 23 is the restriction clause of the GDPR. The first paragraph lays down the conditions under which a Member State can restrict the scope of the obligations that ensue from the data protection principles as laid down in art. 5 GDPR in so far as these principles correspond to the rights and obligations provided for in art. 12 to 22 GDPR. This list of restrictable obligations and rights is exhaustive and should be interpreted strictly and in light of the fundamental rights enshrined in the ECHR and Charter.[633] The non-incompatibility requirement is not further detailed in art. 12 to 22 GDPR; neither is the purpose specification requirement, nor are the fairness-, lawfulness-, and integrity and confidentiality principles.[634] There are, notwithstanding, data protection principles that do correspond with rights and obligations that are detailed in art. 12 to 22 GDPR. There are, firstly, the data minimization- and storage limitation principles ex art. 5(1)(c) and (e) GDPR, that are set forth in the right to erasure and restrictions on processing ex art. 17 and 18 GDPR. Secondly, the transparency principle ex art. 5(1)(a) GDPR is particularized in the information obligations of the data controller and the information- and access rights of the data subject ex art. 12 to 15 GDPR. Lastly, the principle of accuracy ex art. 5(1)(d) GDPR echos in the erasure- and rectification- rights and obligations of art. 16 and 17 GDPR. This group of obligations and rights can be restricted based on art. 23(1) GDPR. The legislative

[632] See for example [Jasserand, 2018, p. 154].

[633] CJEU 7 November 2013, C-473/12, (*IPI*), par. 30-31; CJEU 24 November 2011, C-468/10, (*ASNEF*), par. 34-35;CJEU 20 May 2003, joined cases C-465/00, C-138/01, C-139/01 (*Rechnungshof/Österreichischer Rundfunk and Others, and Christa Neukomm and Joseph Lauermann/Österreichischer Rundfunk*) par. 86; Those restrictions should be in accordance with the requirements set out in the Charter and in the European Convention for the Protection of Human Rights and Fundamental Freedoms. Recital 73 GDPR.

[634] See also CJEU 24 November 2011, C-468/10, (*ASNEF*), par. 35 and 52; and CJEU 20 May 2003, joined cases C-465/00, C-138/01, C-139/01, (*Rechnungshof/Österreichischer Rundfunk and Others, and Christa Neukomm and Joseph Lauermann/Österreichischer Rundfunk*), par. 100.

measures that are taken pursuant to art. 23(1) GDPR will have to meet the criteria of art. 23(2) GDPR, which will be discussed in Section 5.2.1.2 and 5.2.2.2. The analysis of art. 23 GDPR leads, therefore, to the preliminary conclusion that the purpose limitation principle, as well as the accountability-, fairness-, lawfulness-, and integrity and confidentiality principles, cannot be restricted based on that provision because these principles that do correspond with rights and obligations that are detailed in art. 12 to 22 GDPR.

5.2.1.2 Scope of art. 23 GDPR compared to art. 13 DPD in light of art. 8(2) CFREU

The restriction clause of the DPD, art. 13, provided for the restriction of a distinctly different range of data protection principles than art. 23 GDPR does. Article 13 DPD delineated that Member States had the possibility to adopt legislative measures to restrict the scope of the obligations and rights provided for in art. 6(1) DPD, which has laid down the data protection principles, as well as the scope of the data subject rights and data controller obligations that have been laid down in art. 10, 11(1), 12 and 21 DPD.[635] As described in 5.2.1.1, the restriction of the data protection principles is made dependent on them being expressed in other provisions of the GDPR. This was not the case in its precursor, the DPD. It is, therefore, assertable that in the year 1995 it was indeed the legislature's intention to make it possible to restrict all data protection principles that were codified in art. 6 DPD, including the non-incompatibility requirement, under the restriction clause of art. 13 DPD. Twenty-one years later the EU legislature made a different decision and excluded the purpose limitation principle, the fairness- and lawfulness principle, as well as the integrity and confidentiality principle from the restrictable scope of art. 23 GDPR. To this extent the protection that is guaranteed under EU data protection law has been increased.

This set of excluded principles corresponds to a large extent with the elements of the first sentence of art. 8(2) CFREU, which elucidate the fundamental right to protection of personal data ex art. 8(1) CFREU. That sentence lays down that personal data must be processed *fairly*, for *specified purposes* and *lawfully*, either on the basis

[635] There are more differences than just the scope. E.g. only the requirements of legality and necessity was laid down in the DPD and in the GDPR it is legality, necessity, proportionality and essence of the rights. Also the objectives are more varied under the GDPR than under the DPD.

of the consent of the person concerned or on some other legitimate basis laid down by law.[636] From the set of principles that is excluded from the restriction scope of art. 23(1) GDPR, art. 8(2) CFREU is missing the non-incompatibility requirement of the purpose limitation principle as well as the integrity and confidentiality principle, that lays down that personal data must be "processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures."[637]

The significance of the latter principle has been, however, underlined by the CJEU when it interpreted the essence of the right to protection of personal data ex art. 8(1) CFREU in light of the integrity and confidentiality principle.[638] In Section 4.2.4 the *Canada-EU PNR*-opinion has been discussed. In this Opinion the CJEU connected the principle of integrity and confidentiality to the essence of the fundamental right to protection of personal data.[639] What is more, the purpose specification requirement is also connected to the essence of the right to protection of personal data.[640] These findings suggest that the data protection principles can de divided into three groups: Firstly, the set of principles that can be restricted under art. 23(1) GDPR, consisting of the data minimization-, storage limitation-, transparency- and accuracy principles, which were discussed in Section 5.2.1.1. Secondly, the group of principles that cannot be restricted under art. 23(1) GDPR and that are linked to the fundamental right to protection of personal data, either through a direct reference as a principle in the text of the first sentence of art. 8(2) CFREU or through a linkage to the essence of the fundamental right to protection of personal data ex art. 8(1) CFREU made by the CJEU. This group comprises of the purpose specification requirement of the purpose limitation principle, the fairness- and lawfulness principle, and the integrity and confidentiality principle. Thirdly, the group that cannot be restricted under art. 23(1)

[636] See Section 2.1.2.4 on page 40 about the different rights and data protection principles that are detailed in article 8 CFREU.

[637] Article 5(1)(f) GDPR.

[638] Opinion CJEU (Grand Chamber), 8 September 2016, ECLI:EU:C:2016:656, *(Opinion on the Draft Agreement between Canada and the European Union 1/15)*.

[639] Opinion CJEU (Grand Chamber), 26 July 2017, ECLI:EU:C:2017:592, (*Opinion on the Draft Agreement between Canada and the European Union 1/15*), par. 150.

[640] This aspect is discussed at more length in Section 4.2.4 on page 124; Opinion CJEU (Grand Chamber), 26 July 2017, ECLI:EU:C:2017:592, (*Opinion on the Draft Agreement between Canada and the European Union 1/15*), par. 150.

GDPR and is not connected to the fundamental right to protection of personal data: the non-incompatibility requirement of the purpose limitation principle.

5.2.2 The legal framework for re-use based on the *lex specialis* derogation of art. 6(4) GDPR

The following section discusses the specific derogation clause of art. 6(4) GDPR that foresees is the enactment of a *lex specialis* rule and compares the safeguards of art. 6(4) GDPR to those of art. 23 GDPR and assesses these safeguards in light of fundamental rights. This is section describes an other type of use limitation in data protection law and therefore answers the subquestion: What other types of limitations on data processing are implemented in European data protection law?

5.2.2.1 An exclusive derogation clause for the non-incompatibility requirement

Derogations can be made to special category of data protection principles that is not restrictable under the art. 23 GDPR and is not associated with the fundamental right to protection of personal data ex art. 6(4) GDPR. Article 6(4) GDPR delineates that a compatibility test should be conducted where the processing for a purpose other than that for which the personal data have been collected is not based on renewed consent or a *lex specialis* that meets the criteria stemming from fundamental rights law. This passage lifts the rule of cumulation, which is discussed in Section 3.5 on page 79, between the non-incompatibility requirement of the purpose limitation principle and two lawful processing grounds: consent and a legislative measure. Re-use based on renewed consent is discussed in Section 5.3. This Section discusses further processing of data for incompatible purposes that is:

- based on a Union or Member State law;
- necessary and proportionate; and
- in pursuance of a legitimate objective as exhaustively listed in art. 23(1)(a) to (j) GDPR.

It is apparent from the text of art. 6(4) GDPR that the EU legislature intended to give the Member States the freedom to decide whether, and if so for what purposes, they wish to take legislative measures aimed at re-use of personal data for the

objectives of 23(1) GDPR.[641] This is also underlined in Recital 10 of the GDPR that lays down that for processing of personal data for compliance with a legal obligation, Member States should be allowed to maintain or introduce national provisions to further specify the application of the rules of this Regulation.[642] The structure of the GDPR dictates that restrictions of the data protection principles, that were discussed in Section 5.2.1.1 and which are based on the general restriction clause of art. 23 GDPR, should not be the rule and require to be an exception.[643] This is, however, different for further processing for incompatible purposes, which is placed in art. 6 GDPR, that titles *Lawfulness of processing*. The position of the provision normalizes re-use of data to a greater extent than the extent to which it was acceptable under the DPD where the restriction of the non-incompatibility requirement was placed under the general restriction clause for rights and obligations, as explained in Section 5.2.1.2 on page 154.

5.2.2.2 Comparison between the *lex specialis* derogation of art. 6(4) and art. 23 GDPR

Both the article 23 GDPR and art. 6(4) GDPR requirements refer to the justification criteria stemming from fundamental rights: legality, legitimate aim, and necessity and proportionality. These references bring a high level of protection into the secondary data protection framework, because the requirements apply regardless of whether the derogation or restricting measure restricts only a rule from secondary data protection law or restricts the fundamental rights protected in particular in art. 7 CFREU and art. 8 ECHR. The art. 8(1) ECHR assessment on the establishment of an interference and its impact can, therefore, be skipped when measures are taken pursuant to art. 6(4) or 23 GDPR. The art. 23(1) GDPR restriction clause also invokes the concept of respect for the essence of the right. This, however, does not aid the protection

[641] The CJEU argued in similar fashion about freedom of the Member States to decide whether, and if so for what purposes, they wish to take legislative measures aimed at limiting the rights of the data subjects, inter alia, limit the extent of the obligations of the data controller. CJEU 29 January 2008, C-275/06, (*Productores de Música de España (Promusicae)/Telefónica de España SAU*), par. 50-53; CJEU 7 November 2013, C-473/12, (*IPI*), par. 32; This is different for the obligations to adopt legislative measures that reconcile journalism with data protection. CJEU 7 November 2013, C-473/12, (*IPI*), par. 33 and 37.

[642] Recital 10 GDPR.

[643] CJEU 21 December 2016, C-203/15 and C-698/15 (*Tele2 Sverige/Post- och telestyrelsen* and *Secretary of State for the Home Department/Tom Watson, Peter Brice, Geoffrey Lewis*), par. 104.

of fundamental rights neither does it increase the level of protection in secondary data protection law. Because the applicability of the GDPR implies applicability of the CFREU, all data processing must respect the essence of the right to privacy and protection of personal data ex art. 7 and 8 juncto art. 52(1) CFREU. Repeating this in secondary law does not add to the protection. The requirements of the derogation clause of art. 6(4) GDPR and the restriction clause of art. 23(1) GDPR are in this degree similar.

Nevertheless, the regime of art. 6(4) GDPR is different from the procedure of art. 23(1) GDPR to the extent that the second paragraph of art. 23 GDPR does not apply to further use of data for incompatible purposes. That paragraph lays down the minimum criteria that the legislature has to put down in law when taking measures pursuant to art. 23(1) GDPR. See the list on page 152. The legislature is, for example, obligated to determine and codify in law the retention periods and the categories of personal data that are involved in the measures that are based on art. 23(1) GDPR.

Legislative measures that are based on art. 6(4) GDPR have to meet the requirements from art. 6(1)(c) and art. 6(3) GDPR, which match with the art. 23 GDPR requirements to a large extent. Similar to art. 23(2), art. 6(3) GDPR obligates the legislature to determine the purposes of further use in the legislative measure. However, all other requirements from art. 6(3) GDPR are voluntary and should be considered suggestions of the EU legislature to itself or the National legislature.[644] For example, art. 6(4) juncto 6(1)(c) and 6(3) do not obligate the legislature to codify and communicate via law the retention periods and categories of personal data that are being further processed for incompatible purposes. Such characteristics of the further processing can be determined and communicated in a privacy policy ex art. 14 GDPR. The democratic oversight on derogations on the non-incompatibility requirement of the purpose limitation principle is therefore less far-reaching than it is on restrictions on other data protection principles. The only obligatory aspect that has to be codified in Union or Member State law is the purposes specification, which underlines the central importance of the purpose specification requirement to the right to protection of personal data and its association with the essence to that right.

Further processing pursuant to a *lex specialis* that is based on art. 6(4) juncto art. 23(1) GDPR is considered a new processing operation that on its own merits will

[644] Article 6(3) GDPR puts down that the legal basis *may* contain specific provisions to adapt the application of rules of this Regulation.

have to meet the four cumulating data protection touch stones.[645] The provisions of art. 6(4) juncto art. 23(1)(a) to (j) GDPR lay down the criteria that have to be met by a legislative measure – the *lex specialis* – that provides for re-use of personal data. These GDPR provisions itself do not provide the legal base for the re-use. The objectives listed in art. 23(1) GDPR include re-use of data that would fall outside the scope of EU law, re-use that would fall under the scope of the GDPR and re-use of data that would fall under the scope of the LED. The latter is specified in art. 23(1)(d) GDPR, which stipulates the objective of the prevention, investigation, detection or prosecution of criminal offenses or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security. Given the rationale of this study – purpose limitation and the detection of crime – the re-use for objectives that fall under that subsection are further investigated.[646]

5.2.2.3 The *lex specialis* derogation of art. 6(4) GDPR in light of fundamental rights protection

Recital 73 GDPR explains that the art. 23 GDPR restrictions should be in accordance with the requirements set out in the Charter and in the European Convention for the Protection of Human Rights and Fundamental Freedoms. This figure of *protective presumptions* can be observed in more data protection law. The ePrivacy Directive, for example, obligates the data controller to obtain consent from the user before a cookie is dropped and without having to assess if the cookie should be considered personal data as defined under the DPD. A similar explanation of the interpretation of the con-

[645] See Section 3.5 on page 79.

[646] With regard to re-use for objectives that fall outside the scope of EU law future research is recommended. For re-use for objectives that would fall under the GDPR the processing ground for the further use is a Union or Member State law to which the controller is subject as is referred to in art. 6(1)(c) juncto art. 6(3)(a) and (b) GDPR. The latter provision lays down that the processing purposes must be determined in that legal basis and meet an objective of public interest and be proportionate to the legitimate aim pursued. The last passage of Art. 6(3) GDPR suggests volitional specific provisions for laws that are adopted pursuant to art. 6(1)(c) GDPR to adapt the application of rules of the GDPR. The provision recommends including in the legislative measure: the general conditions governing the lawfulness of processing by the controller; the types of data which are subject to the processing; the data subjects concerned; the entities to, and the purposes for which, the personal data may be disclosed; the purpose limitation; the retention periods; and the processing operations and processing procedures, including measures to ensure lawful and fair processing for specific processing situation such as processing for privileged purposes. With regard to the latter: See Section 5.6 on page 189.

cepts of art. 6(4) GDPR is missing in the recitals of the GDPR. Be that as it may, for this study the requirements are explained in light of the fundamental rights doctrine, because, firstly, the vocabulary in the derogation clause is that of the fundamental rights framework, secondly, the DPC obligates States to apply the fundamental rights criteria for derogations of data protection principles, and thirdly, as discussed in Section 5.1.3, the further processing of GDPR-data for LED purposes easily interferes with the fundamental rights as protected in art. 7 CFREU and art. 8(1) ECHR.

5.2.2.3.1 Legitimate aim For data processing that falls under the scope of the GDPR the objectives of general interest recognized by the Union are further stipulated in art. 23(1) GDPR, which is referred to in art. 6(4) GDPR. In the context of this study the most relevant objectives are the prevention, investigation, detection or prosecution of criminal offenses or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security ex art. 23(1)(d) GDPR, national- and public security ex art. 23(1)(a) and (c) GDPR, and the rights and freedoms of others ex art. 23(1)(i) GDPR.[647]

The Luxembourg- and Strasbourg Courts do not have a tradition of elaborate reasoning on the notion of legitimate aims or objectives, specifically not when a measure

[647] The full list of Article 23(1) includes: *a.* national security; *b.* defense; *c.* public security; *d.* the prevention, investigation, detection or prosecution of criminal offenses or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security; *e.* other important objectives of general public interest of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, including monetary, budgetary and taxation a matters, public health and social security; *f.* the protection of judicial independence and judicial proceedings; *g.* the prevention, investigation, detection and prosecution of breaches of ethics for regulated professions; *h.* a monitoring, inspection or regulatory function connected, even occasionally, to the exercise of official authority in the cases referred to in points (a) to (e) and (g); *i.* the protection of the data subject or the rights and freedoms of others; and *j.* the enforcement of civil law claims. The DPD left uncertainty with regard to the legitimacy of processing for the objective of art. 23(1)(h) GDPR. The CJEU decided in that regard that "since Directive 95/46 does not specify the manner in which the investigation and detection of failures to comply with the rules are carried out, it must be considered that the directive does not prevent such a professional body from having recourse to specialized investigators, such as private detectives responsible for that investigation and detection, in order to perform its duties". CJEU 7 November 2013, C-473/12, (*IPI*), par. 44-45; For data processing for the purpose of safeguarding the public security it should be noted that with regard to the latter objective, art. 6 of the CFREU plays a significant role when data is processed for purposes of public security, because that article lays down the right of any person to liberty and security.

is deemed to be in pursuance of such aim. Odd ones out with the ECtHR are cases that concern database registrations of sex offenders.[648] In the inadmissibility decision of in the *Adamson*-case, for example, the ECtHR regards the British database registration of a former sex offender to contribute towards the legitimate aim of a lower rate of reoffending and therefore to the prevention of crime. The personal data was processed for the purposes of increasing the data subject's awareness of being registered with the police in hope that this may dissuade her from committing further offenses and for the purpose of enabling the police to trace suspected reoffenders faster.[649] The ECtHR considered that the data processing for these purposes pursues the legitimate aims of the prevention of crime and the protection of the rights and freedoms of others.[650]

There is some case law in which the ECtHR determined a violation of art. 8 ECHR because the disputed measure lacked legitimate aim. These cases concerned the publication of data relating to private life by the press. In these cases the further processing of the data in a different context than the initial context of data collection led to the admissibility of the complaints in Strasbourg. For example, the *Biriuk*-case about the publication of a tabloid-style news article concerning the HIV infection of a person.[651] The main purpose of the publication was to increase the newspaper sales. In the ECtHR's view "the publication of the article in question, the purpose of which was apparently to satisfy the prurient curiosity of a particular readership and boost [...] commercial interests, cannot be deemed to contribute to any debate of general

[648] ECtHR 26 January 1999, no. 42293/98 (*Adamson/the United Kingdom*), part 1; ECtHR 17 December 2009, no. 16428/05 (*Gardel/France*); ECtHR 17 December 2009, no. 5335/06 (*Bouchacourt/France*)

[649] ECtHR 26 January 1999, no. 42293/98 (*Adamson/the United Kingdom*), part 1.

[650] ECtHR 26 January 1999, no. 42293/98 (*Adamson/the United Kingdom*), part 2. Ten years later the ECtHR investigates the legitimacy of the French sex offenders database. ECtHR 17 December 2009, no. 16428/05 (*Gardel/France*); ECtHR 17 December 2009, no. 5335/06 (*Bouchacourt/France*); ECtHR 17 December 2009, no. 2115/06 (*M.B./France*). The ECtHR acknowledges that the aim of such a register "is to prevent crime and in particular to combat recidivism and, in such cases, to make it easier to identify offenders". Taken into account the safeguards put in place in the French domestic law, the ECtHR deems the infringement not disproportionate to the aim pursued. The ECtHR considered that the applicant's placement on the Sex Offenders Register struck a fair balance between the competing private and public interests at stake and that the respondent State did not overstep the acceptable margin of appreciation in that regard. Accordingly, there had been no violation of Article 8 of the Convention by storing the information in the sex offenders database. ECtHR 17 December 2009, no. 16428/05 (*Gardel/France*), par. 63, 70-71.

[651] ECtHR 25 November 2008, no. 23373/03 (*Biriuk/Lithuania*).

interest to society".[652] The measure lacked a legitimate aim and the Lithuanian domestic legal framework failed to provide for effective remedies resulting in a failure to secure the right to respect for private life of the person that was the subject of the publication.[653] In the *Karajanov*-case the ECtHR concluded in similar fashion that the disputed measure did not pursue legitimate aim. Again in this case, the data was collected in a different context than the context in which it was further used. During the Macedonian lustration process,[654] a Commission decision concerning a citizen's collaboration with the former regime's security services had been published before it had become final.[655] The Government submitted that the publication of such information ensured greater transparency, public access to documents in the applicant's file and public scrutiny of the Commission's decision-making. The ECtHR was not convinced by these arguments and explained that neither purpose can be subsumed under any of the aims listed in Article 8(2) of the Convention. The ECtHR did not see how making a non-final Commission decision publicly accessible can be reconciled with the general aims of lustration.[656] Inevitably, the lack of a legitimate aim lead to a violation of art. 8(2) ECHR.[657]

5.2.2.3.2 Legality In Section 5.2.2.2 of this study I discussed secondary data protection law and the voluntary nature of the codification of data processing details into Union or Member State law when data is being re-used based on art. 6(4) juncto 6(1)(c) and 6(3) GDPR. In this section I discuss the codification requirements of data protection safeguards that are developed by the ECtHR in light of the criterion of *in accordance with the law* and the CJEU in light of the criterion *provided for by law* for data processing in the pre-crime phase of criminal investigations that include secret measures of surveillance. The concept *law* refers to written and unwritten law[658] and requires an infringing measure to have some basis in domestic law as well as to be

[652] ECtHR 25 November 2008, no. 23373/03 (*Biriuk/Lithuania*), par. 42-44.
[653] ECtHR 25 November 2008, no. 23373/03 (*Biriuk/Lithuania*), par. 46-47.
[654] Lustration refers to the purge of government officials once characteristic of the Communist system in Central and Eastern Europe. See [Letki, 2002] for more information on the lustration and democratization of East-Central Europe.
[655] ECtHR 06 April 2017, no. 2229/15 (*Karajanov/the former Republic of Macedonia*), par. 74.
[656] ECtHR 06 April 2017, no. 2229/15 (*Karajanov/the former Republic of Macedonia*), par. 75.
[657] ECtHR 06 April 2017, no. 2229/15 (*Karajanov/the former Republic of Macedonia*), par. 76.
[658] ECtHR 26 April 1979 , no.6538/74 (*Sunday Times/the United Kingdom*) par. 47.

compatible with the Rule of Law.[659] Compatibility with the Rule of Law is expressly mentioned in the Preamble to the ECHR and is inherent in the object and purpose of art. 8 ECHR. Overall, the ECtHR discusses the Rule of Law indirectly in its appraisal of the *quality of the law*.[660] This latter criterion oversees that any infringing measure needs to be accessible, foreseeable[661] and accompanied by necessary procedural safeguards affording adequate legal protection against arbitrary application of the relevant legal provisions.[662] The ECtHR does not interpret the expression *in accordance with the law* as meaning that the safeguards must be enshrined in the very text which authorizes the imposition of restrictions.[663] The ECtHR also closely links the question of safeguards against abuse to the question of effective remedies and sometimes finds it preferable to take that issue into account in the wider context of Article 13 ECHR, that safeguards the right to an effective remedy.[664]

However, the greater the scope of the data collection, and thus the greater the amount or the sensitivity of data that is processed, the more important the implementation of adequate and effective safeguards is at the various stages of the processing.[665] Because data processing technology is continually becoming more sophisticated, safeguards against abuse in clear and detailed rules are, in the view of the ECtHR, essential to automated data processing, particularly when data is fur-

[659] ECtHR 25 March 1983, no. 5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75, 7136/75) (*Silver and Others/the United Kingdom*), par. 90.

[660] ECtHR 24 April 1990, no. 11801/85 (*Kruslin/France*) par. 33; ECtHR 24 April 1990, 4, no.11105/84 (*Huvig/France*) par. 32; ECtHR 2 August 1984, no. 8691/79 (*Malone/the United Kingdom*) par. 67; ECtHR 4 May 2000, no. 28341/95 (*Rotaru/Romania*), par. 55; ECtHR 16 February 2000, no. 27798/95 (*Amann/Switzerland*), par. 56; ECtHR 4 December 2015, no. 47143/06 (*Roman Zakharov/Russia*), par. 228.

[661] ECtHR 26 March 1987, no. 9248/81, (*Leander/Sweden*) par. 50; ECtHR 2 August 1984, no. 8691/79 (*Malone/the United Kingdom*) par. 66.; ECtHR 4 December 2015, no. 47143/06 (*Roman Zakharov/Russia*), par. 228; In the *Amann*-case the Court added that a rule is *foreseeable* if it is formulated with sufficient precision to enable any individual – if need be with appropriate advice – to regulate her conduct. ECtHR 16 February 2000, no. 27798/95 (*Amann/Switzerland*), par. 56.

[662] See for example ECtHR 2 August 1984, no. 8691/79 (*Malone/the United Kingdom*) par. 67; ECtHR 4 December 2008, no.130562/04 and 30566/04 (*S. and Marper/the United Kingdom*), par. 95; ECtHR 18 May 2010, no. 26839/05 (*Kennedy/the United Kingdom*), par. 151; ECtHR 7 July 2015, no. 28005/12 (*M.N. and others/San Marino*), par. 72; ECtHR 4 December 2015, no. 47143/06 (*Roman Zakharov/Russia*), par. 228; and ECtHR 4 May 2000, no. 28341/95 (*Rotaru/Romania*), par. 52.

[663] ECtHR 25 March 1983, no. 5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75, 7136/75) (*Silver and Others/the United Kingdom*), par. 90.

[664] ECtHR 25 March 1983, no. 5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75, 7136/75) (*Silver and Others/the United Kingdom*), par. 90.

[665] ECtHR 13 November 2012, no. 24029/07 (*M.M./the United Kingdom*) par. 200.

ther processed for LED purposes or is collected by surveillance or covert intelligence gathering.[666] The EctHR took various data protection principles into account when it considered that domestic law should, in particular, ensure that the data is relevant and not excessive in relation to the purposes for which it is stored and that the data is preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which that data is stored.[667] In the *Cemalettin Canli*-case the ECtHR regarded the accuracy principle. The cases surrounded a file that contained false information and important information was not added by competent authorities before the file was shared with a third party. In the view of the ECtHR, these failures were due to a lack of a number of substantial procedural safeguards provided by domestic law for the protection of the applicant's rights under Article 8 of the Convention.[668]

When measures are applicable to the general public, these measures have to be sufficiently clear in their terms to give an adequate indication of the circumstances in which and the conditions on which the competent authorities are empowered to process the data.[669] The appropriate level of foreseeability differs from context to

[666] ECtHR 25 March 1998, no. 23224/94 (*Kopp/Switzerland*), par. 71; and ECtHR 16 February 2000, no. 27798/95 (*Amann/Switzerland*), par. 56; ECtHR 17 December 2009, no. 16428/05 (*Gardel/France*), par. 62; ECtHR 13 November 2012, no. 24029/07 (*M.M./the United Kingdom*), par 195; ECtHR 6 June 2016, no.37138/14 (*Szabó and Vissy/Hungary*), par. 73.ECtHR 24 April 1990, no. 11801/85 (*Kruslin/France*), par. 33; ECtHR 24 April 1990, 4, no.11105/84 (*Huvig/France*), par. 32; ECtHR 28 June 2007, no. 62540/00 (*Association for European Integration and Human Rights and Ekimdzhiev/Bulgaria*), par 75; ECtHR 29 June 2006, no. 54934/00 (*Weber and Saravia/Germany*), par 93; ECtHR 4 December 2015, no. 47143/06 (*Roman Zakharov/Russia*), par. 229.

[667] ECtHR 17 December 2009, no. 16428/05 (*Gardel/France*), par. 62; ECtHR 6 June 2016, no.37138/14 (*Szabó and Vissy/Hungary*), par. 73.

[668] ECtHR 18 November 2008, no. 22427/04 (*Cemalettin Canli/Turkey*), par. 42.

[669] ECtHR 2 August 1984, no. 8691/79 (*Malone/the United Kingdom*) par. 67; ECtHR 26 March 1987, no. 9248/81, (*Leander/Sweden*) par. 51; ECtHR 4 May 2000, no. 28341/95 (*Rotaru/Romania*), par. 55; ECtHR 24 April 1990, 4, no.11105/84 (*Huvig/France*), par 29. In the *Uzun*-case the Court stated, in the context of Article 7 of the Convention, "that in any system of law, including criminal law, however clearly drafted a legal provision may be, there is an inevitable element of judicial interpretation. There will always be a need for elucidation of doubtful points and for adaptation to changing circumstances. Indeed, in the Convention States, the progressive development of the criminal law through judicial law-making is a well entrenched and necessary part of legal tradition. The Convention cannot be read as outlawing the gradual clarification of the rules of criminal liability through judicial interpretation from case to case, provided that the resultant development is consistent with the essence of the offence and could reasonably be foreseen". ECtHR 2 September 2010, no. 35623/05 (*Uzun/Turkey*), par. 62.

context. In the special context of secret measures of surveillance, foreseeability does not mean that an individual should be able to exactly foresee when the authorities are likely to access their data or intercept their communications to the extent that she can adapt her conduct accordingly.[670] However, where the power vested in the competent authorities is exercised in secret, the risk of arbitrariness is palpable.[671]

The execution of secret measures, like secret database surveillance with the help of private entities that voluntarily transfer bulk data sets to competent authorities for the detection of crime, is not open to scrutiny by the data subjects concerned or the public at large. In secret measures the discretion granted to the competent authorities and even to a judge should not be expressed in terms of unfettered power, because that would be contrary to the Rule of Law, according to the ECtHR.[672] In such cases the restricting measure should indicate the scope of discretion conferred on the competent authorities as well as the manner of its exercise with sufficient clarity, having regard to the legitimate aim of the measure in question.[673]

In its case law on secret measures of surveillance the ECtHR has developed a set of minimum safeguards that should be implemented in law in order to avoid arbitrary interferences and abuses of power.[674] At first these safeguards were developed in the relation with surveillance measures targeting specific individuals, but over the years the ECtHR applied the safeguards to general programs of surveillance too.[675] The ECtHR saw no need in developing different principles concerning the accessibility

[670] In the *Leander*-case, for example, the ECtHR explained that "foreseeability in the special context of secret controls of staff in sectors affecting national security cannot be the same as in many other fields. Thus, it cannot mean that an individual should be enabled to foresee precisely what checks will be made in his regard" by the special police service in their efforts to protect national security. ECtHR 26 March 1987, no. 9248/81, (*Leander/Sweden*) par. 51.

[671] ECtHR 2 August 1984, no. 8691/79 (*Malone/the United Kingdom*) par. 86; ECtHR 4 December 2015, no. 47143/06 (*Roman Zakharov/Russia*), par. 229.

[672] ECtHR 4 December 2015, no. 47143/06 (*Roman Zakharov/Russia*), par. 230; ECtHR 6 June 2006, no. 62332/00 (*Segerstedt-Wiberg and others/Sweden*), par. 76; In multiple cases the ECtHR noted that secret surveillance systems – despite if being designed to protect national security – entail the risk of undermining or even destroying democracy on the ground of defending it. ECtHR 4 May 2000, no. 28341/95 (*Rotaru/Romania*) par. 59; ECtHR 6 September 1978, no. 5029/71 (*Klass and others/Federal Republic of Germany*) par. 49.

[673] ECtHR 2 August 1984, no. 8691/79 (*Malone/the United Kingdom*) par. 86.

[674] See for example ECtHR 4 May 2000, no. 28341/95 (*Rotaru/Romania*), par. 57 for a comprehensive example of the Court's assessment.

[675] See for example ECtHR 29 June 2006, no. 54934/00 (*Weber and Saravia/Germany*), par. 18 and 145.

and clarity of the rules governing the interception of individual communications, on the one hand, and more strategic monitoring, on the other.[676]

In the *Weber and Saravia*-case the ECtHR listed these safeguards:[677] Firstly, the law should give clarity as to the nature of the offenses which may give rise to the surveillance.[678] Secondly, a definition of the categories of people liable to be under surveillance should be formulated.[679] Thirdly, a limit on the duration of surveillance should be set.[680] Next, the legislature should specify the nature of the data, the procedure to be followed for collecting, examining, consulting, using and storing the data obtained, the precautions to be taken when data is shared with other parties, and the circumstances in which data may or must be erased.[681] In the *Liberty*-case, which concerned general surveillance, the ECtHR added to this list the procedure to be followed for selecting data for examination.[682] Lastly, the ECtHR takes into account the review and supervision of secret surveillance measures, which comes into play at three stages: when the surveillance is first ordered, while it is carried out and the data is being processed, and after it has been terminated.[683] The nature and logic of secret surveillance dictates that the surveillance itself and the accompanying review procedure should be effective without the subject's knowledge of being under surveillance.

With regard to this supervisory procedures the ECtHR underlined in the *Zakharov*-case that the values of a democratic society must be followed as faithfully as possible.[684] Under the adagio *Who is watching the watchdog?* effective safeguards against

[676] ECtHR 1 July 2008 , no.58243/00 (*Liberty and others/the United Kingdom*), par. 63.

[677] See to this extent also the *Big Brother Watch*-case that is referred to the Grand Chamber. At the moment of finishing this study the outcome is yet unknown. case in first instance: ECtHR 13 September 2018, nos. 58170/13, 62322/14 and 24960/15 (*Big Brother Watch and others/the United Kingdom*).

[678] See for example ECtHR 29 June 2006, no. mai (*Weber and Saravia/Germany*), par. 95.

[679] See also for example ECtHR 16 February 2000, no. 27798/95 (*Amann/Switzerland*), par. 58.

[680] See also for example ECtHR 28 June 2007, no. 62540/00 (*Association for European Integration and Human Rights and Ekimdzhiev/Bulgaria*), par. 76.

[681] See for also example ECtHR 24 April 1990, no. 11801/85 (*Kruslin/France*), par. 35; ECtHR 24 April 1990, no. 11105/84 (*Huvig/France*), par. 34; ECtHR 29 June 2006, no. 54934/00 (*Weber and Saravia/Germany*), par. 95; ECtHR 16 February 2000, no. 27798/95 (*Amann/Switzerland*), par. 76; See similar safeguards in the cases: ECtHR 4 May 2000, no. 28341/95 (*Rotaru/Romania*), par. 57; ECtHR 13 November 2012, no. 24029/07 (*M.M./the United Kingdom*), par. 206; ECtHR 4 May 2000, no. 30194/09 (*Shimovolos/Russia*), par. 69.

[682] ECtHR 1 July 2008 , no.58243/00 (*Liberty and others/the United Kingdom*), par. 69.

[683] See for example ECtHR 4 December 2015, no. 47143/06 (*Roman Zakharov/Russia*), par. 233.

[684] ECtHR 4 December 2015, no. 47143/06 (*Roman Zakharov/Russia*), par. 233. The Court adds that in

abuse of monitoring powers should be established too. This includes notification of the subject after the surveillance is terminated to enable her to challenge the legality retrospectively.[685] What is more, any person who suspects that she is under surveillance should be able to apply to a court of law and the jurisdiction of that court should not depend on the notification of the subject by the competent authorities.[686] When there are no domestic measures in place to challenge the surveillance, the ECtHR has tested *in abstracto* because it was unable for an individual to know whether there has been a concrete interference due to the lack of any sort of notification- or information mechanism in domestic surveillance laws.[687] The ECtHR considers *a posteriori* oversight important because it provides redress for any abuse sustained and has the potential of reinforcing citizens' trust with guarantees that the rule of law is at work even in sensitive fields, like national or public security.[688]

5.2.2.3.3 Necessity and proportionality The ECtHR has considered in multiple cases that the similarity of confidentiality- and data protection regimes within different tranches of government contributes to the legitimacy and proportionality of further processing of data relating to private life for incompatible purposes.[689] However, the *L.H./Latvia*-case made clear that confidentiality safeguards can not substitute for purpose limitation or the overall proportionality of the data processing.[690] In that case the ECtHR explained that it becomes less relevant whether the staff of the data controller had a legal duty to maintain the confidentiality of personal data, when the data controller appeared to have collected the data indiscriminately, without any prior assessment of whether the data collected would be *potentially decisive*, *relevant* or *of importance* for achieving whatever aim might have been pursued by the controller's inquiry.[691] The further use of data for incompatible purposes should also meet the

"a field where abuse is potentially so easy in individual cases and could have such harmful consequences for democratic society as a whole, it is in principle desirable to entrust supervisory control to a judge, judicial control offering the best guarantees of independence, impartiality and a proper procedure."

[685] ECtHR 6 September 1978, no. 5029/71 (*Klass and others/Federal Republic of Germany*), par. 57-58.

[686] See for example ECtHR 18 May 2010, no. 26839/05 (*Kennedy/the United Kingdom*), par. 167, 184-191.

[687] This was for example the case in ECtHR 4 December 2015, no. 47143/06 (*Roman Zakharov/Russia*).

[688] ECtHR 6 June 2016, no.37138/14 (*Szabó and Vissy/Hungary*), par. 79.

[689] For example ECtHR 27 August 1997, no. 20837/92 (*M.S./Sweden*), par. 43; ECtHR 17 December 2009, no. 16428/05 (*Gardel/France*), par. 69-70.

[690] ECtHR 29 April 2014, no. 52019/07 (*L.H./Latvia*).

[691] ECtHR 29 April 2014, no. 52019/07 (*L.H./Latvia*), par. 58.

criterion of subsidiarity: when certain conclusions can be drawn without the re-use of that specific set of data relating to private life, the processing cannot be deemed necessary in a democratic society.[692]

While balancing competing interests, States enjoy a certain margin of appreciation in determining the necessity of a restrictive measure and choosing the means for achieving the legitimate aim, which is subject to the supervision of the ECtHR.[693] This margin embraces the legislation on which the restrictive measure is based, the decisions on applying the measure, and its execution.[694] Its scope depends on factors such as the nature and seriousness of the interests at stake and the gravity of the interference.[695]

For targeted and low-tech surveillance States enjoy a wider discretion,[696] whereas non-specific, general, high-tech or novel surveillance is under strict scrutiny of the ECtHR,[697] even when this is conducted in the interest of national security, a field which is traditionally characterized by a wider margin of appreciation.[698] Secret surveillance powers that can be linked to the characteristics of a police state are, according to the ECtHR, only tolerable in so far as they are strictly necessary for safeguarding the democratic institutions.[699] When it comes to data protection issues outside the field of national security, the margin of appreciation of the States in designing their respective legislative and administrative frameworks is limited.

---

[692] ECtHR 10 October 2006, no. 7508/02 (*L.L./France*), par. 46.

[693] See for an elaborate study on the interpretation and history of this concept: [O'Donnell, 1982] and [Hutchinson, 1999].

[694] ECtHR 22 February 1989, no. 11508/85 (*Barfod/Denmark*), par. 28; ECtHR 9 June 2009, no. 72094/01 (*Kvasnica/Slovakia*), par. 80.

[695] ECtHR 28 January 2003, no. 44647/98 (*Peck/the United Kingdom*), par. 77; ECtHR 17 December 2009, no. 16428/05 (*Gardel/France*), par. 60; With regard to data protection issues, the ECtHR explained that a highly intimate and sensitive nature of data, such as information concerning a person's HIV status, can call for more careful scrutiny on the part of the Court. ECtHR 25 February 1997, no. 22009/93 (*Z/Finland*), par 89 and 99; ECtHR 6 June 2013, no. 1585/09 (*Avilkina/Russia*), par. 46.

[696] ECtHR 6 September 1978, no. 5029/71 (*Klass and others/Federal Republic of Germany*), par. 49; and ECtHR 26 March 1987, no. 9248/81, (*Leander/Sweden*), par. 59.

[697] ECtHR 6 June 2016, no.37138/14 (*Szabó and Vissy/Hungary*), par. 57; ECtHR 4 December 2015, no. 47143/06 (*Roman Zakharov/Russia*), par. 232; ECtHR 4 December 2008, no.130562/04 and 30566/04 (*S. and Marper/the United Kingdom*), par. 112.

[698] The *Weber*-case demonstrated the elasticity of the margin of appreciation, even in a field such as national security. ECtHR 29 June 2006, no. 54934/00 (*Weber and Saravia/Germany*), par. 106.

[699] ECtHR 6 September 1978, no. 5029/71 (*Klass and others/Federal Republic of Germany*), par. 42; ECtHR 6 June 2016, no.37138/14 (*Szabó and Vissy/Hungary*), par. 54.

In the past decades a certain level of consensus on the international level – in particular between the Council of Europe Member States – has been achieved regarding the data protection principles and the corresponding basic procedural safeguards to be included in the national legislative frameworks in order to justify the necessity of any possible interference. The Data Protection Convention, the GDPR and the LED are examples of this. This consensus led to a gradual reduction of the margin of appreciation of States in the ECtHR rulings that concerned data protection issues in the past years, which the ECtHR underlined in the *Sukirov*-case in 2017.[700] In 1998, almost 20 years ahead of his time, Bygrave foresaw this and already argued that the existence of the Data Protection Convention and the DPD, represented a common set of European data protection principles and that, therefore, the margin of appreciation of the Contracting States should ultimately be limited in data protection issues.[701]

The necessity of further processing of data that would fall under the scope of the GDPR is predominantly discussed by the ECtHR in relation to health data. For this group of cases the ECtHR regards a change in processing purposes necessary in a democratic society when the processing is subject to limitations and accompanied by effective and adequate safeguards against abuse.[702] Consent of the data subject and limited dissemination of the data play an important role in the process of determining the proportionality of the interference.[703] The *Surikov*-case demonstrates the ECtHR reasoning nicely.[704] In this case a complaint was filed by an employee of a State-owned company regarding his long-awaited but continuously postponed promotion at work. His promotion requests were dismissed by the employer on grounds of the mental health of the employee from a few years back which the employer learned from reports that were made years prior to his employment and that were initially intended to grant the employee dispensation from military service in peacetime. Under Ukrainian law the reports were lawfully shared with the employer. The ECtHR noted that the national law essentially resulted in a quasi-automatic entitlement for any employer, whether public or private, to obtain and retain sensitive health-related data concerning any employee dispensed from military service on medical grounds.[705] The

[700] ECtHR 26 January 2017, no. 42788/06 (*Surikov/Ukrain*), par. 74.
[701] [Bygrave, 1998, p. 273].
[702] ECtHR 27 August 1997, no. 20837/92 (*M.S./Sweden*) par. 43.
[703] ECtHR 27 August 1997, nr. 20837/92 (*M.S./Sweden*) par. 43; ECtHR 6 June 2013, no. 1585/09 (*Avilkina/Russia*), par. 48.
[704] ECtHR 26 Januari 2017, no. 42788/06 (*Surikov/Ukrain*).
[705] ECtHR 26 Januari 2017, no. 42788/06 (*Surikov/Ukrain*), par. 76 and 86.

law put down a long retention period and also authorized further processing of the data for purposes that were not related to the initial purpose of data collection. The ECtHR explained that the processing of sensitive health-related data concerning employees can only be justified under art. 8 ECHR when particularly strong procedural guarantees are provided, such as confidentiality, purpose limitation and accuracy of the data.[706]

For the topic of this study the conclusions from the *Avilkina/Russia*-case are of interest too.[707] In that case the public prosecutor collected information about the applicant for the investigation of a crime of which the applicants were no suspects. The public prosecutor conducted an investigation into the religious group of the applicants and collected their medical files without priorly consulting the applicants, let alone ask them for consent. The ECtHR considered the question of wether or not the person to whom the data relates is subject to criminal law investigations or is accused in any criminal investigation important to the assessment of the necessity of the interference. The Court concluded that the collection of the data by the prosecution office was not accompanied by sufficient safeguards to prevent disclosures inconsistent with the right to respect for private life ex art. 8 ECHR.[708] In this case there was a link between the suspect and the applicants. In data-driven crime detection there is potentially no link because the criminal law enforcement authorities have not yet identified a crime or a suspect.

5.2.3 Conclusion on re-use based on a *lex specialis* as required in art. 6(4) GDPR

Re-use based on a *lex specialis* as required in art. 6(4) GDPR must meet the justification criteria stemming from fundamental rights. The derogations of the rule to cumulation have been part of fundamental data protection law since the first international data protection rules. Processing based on such a derogation is considered a new processing instance. This system of derogations is supported by the case law of the ECtHR because from the analyzed cases we can conclude that incompatibility *per se* has never lead to an infringement.

[706] ECtHR 26 Januari 2017, no. 42788/06 (*Surikov/Ukrain*), par. 76, 86-94.
[707] ECtHR 6 June 2013, no. 1585/09 (*Avilkina/Russia*).
[708] ECtHR 6 June 2013, no. 1585/09 (*Avilkina/Russia*), par. 47-48.

5.3 Re-use based on renewed consent ex art. 6(4) juncto 6(1)(a) GDPR

This section discusses the second derogation from the rule of cumulation: re-use based on consent. This is the second different type of use imitation that is discussed in this study.

Where data is collected under the GDPR and the data controller wishes to further process this data for new purposes that do not pass the compatibility test, the data subject can give her consent to the processing for the new specified purposes.[709] The EDPB refers to this type of consent as *downstream consent*,[710] and the CJEU uses the term *renewed consent*, to which I will stick.[711] It is important to recognize that the cumulation rule is lifted only for the non-incompatibility requirement and not for the purpose limitation principle as a whole.[712] Data processing based on renewed consent cannot waive the obligation for the data controller to specify the processing purposes prior to the processing or bargain limited liability because the other data protection principles still apply.[713]

In renewed consent situations the data controller is not limited in the type of processing purposes,[714] as she is in the case for re-use based on the art. 6(4) GDPR juncto art. 6(1)(c) because the processing purposes must fulfill one of the objectives listed in art. 23(1) GDPR.[715] Also, contrary to re-use based on art. 6(4) juncto 23(1) GDPR, which require a foreseeability assessment in the proportionality assessment, the data controller is not held to assess the necessity and proportionality of the new processing purposes in light of the initial purposes when renewed consent can be obtained.

[709] Article 6(4) GDPR; Article 29 Working Party *Opinion on Purpose Limitation*, 2013, WP 203, p. 3; For in an in-depth study of consent in data protection law see [Kosta, 2013a]; Renewed consent has been part of the data protection corpus since the OECD guidelines that were adopted in the year 1980, which is discussed in footnote 2.2 on page 45.

[710] Article 29 Working Party *Opinion 15/2011 on the definition of consent*, 2011, WP 187, p. 19.

[711] CJEU15 May 2011, C-543/09, (*Deutsche Telekom AG/Germany*).

[712] This is similar to further use of data for privileged purposes which will be discussed in Section 5.6.

[713] See Section 3.3 on page 61 of this study on the elements of purpose limitation.

[714] The type limitation that does exist is that new processing purposes should fall in the category of legitimate purposes. See Section 3.3.2 on page 64 on this topic; For further use for privileged purposes the data controller is bound to the type of purposes. See Section 5.6. Similarly, in the case re-use of data for privileged purposes which will be discussed in Section 5.6.

[715] See Section 5.2.2.

Data processing that is based on renewed consent qualifies as a new data processing operation that has to meet the four cumulating data protection touchstones on its own merits.[716] This also includes making sure that the data subject's renewed consent meets the conditions to qualify as a lawful freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing ex art. 7 GDPR and Recital 32, 42 and 43 GDPR.[717] The latter recital explains that consent cannot provide a valid legal ground for the processing of personal data in a specific case where there is a clear imbalance between the data subject and the controller, in particular where the controller is a public authority and it is therefore unlikely that consent was freely given in all the circumstances of that specific situation.[718]

5.4 Further use of GDPR-data for LED purposes ex Recital 50 GDPR

The following sections describe the interaction between the LED and the GDPR when GDPR-data is further used for purposes that pursue LED objectives. This section contributes to the answer to the subquestion: How are voluntary data transfers of GDPR-data for LED objectives regulated in the European data protection framework?

5.4.1 The attempt to regulate data flows from private entities operating under the GDPR to competent authorities operating under the LED

At one moment in time during the legislative process of the new regulatory framework, the EU Parliament proposed a specific article for the access of competent authorities to data that is collected for purposes other than those referred to in art. 1(1) LED, for example for data that was collected under the regime of the GDPR or for purposes that fall outside the scope of EU law.[719] That proposed provision made a

[716] See Section 3.5 on page 79 of this study.

[717] Consent covers all aspects of processing relating to the fulfillment of a purpose, including for example the passing of personal data to another undertaking of the data controller and processing for the same purpose but with different means. CJEU 15 May 2011, C-543/09, (*Deutsche Telekom AG/Germany*), par. 65.

[718] See in this regard also the Article 29 Working Party *Opinion on Consent*, 2011, WP 187.

[719] Amendment 63, Article 4a, Access to Data Initially Processed for Purposes Other Than Those Referred to in Art. 1(1), European Parliament legislative Resolution on the protection of individuals with regard to

distinction between, on the one hand, access to data held by criminal law enforcement authorities for other purposes than those referred to in art. 1(1) LED. For this category the proposal allowed access to that data in a specific case, and when reasonable grounds gave reason to believe that the processing of the personal data will substantially contribute to the prevention, investigation, detection or prosecution of criminal offenses or the execution of criminal penalties. For personal data held by private parties or other public authorities, the proposal only permitted access for the investigation and prosecution of criminal offenses in a specific case and in accordance with necessity and proportionality requirements to be defined by Union law or Member State law. This amendment proposed some serious constraints on public-private partnerships because disclosures for the detection of crime were excluded.

The amendment did not make it to the final text of the LED.[720] The European Commission was not in favor of a specific provision for further use of initial non-LED-data under the LED and stated that "further processing across the two legal instruments would create problems and that there were no specific Articles to be used for that."[721]

---

the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offenses or the execution of criminal penalties, and the free movement of such data COM(2012)0010- C-7-0024/2012-2012/010(COD) P7_TA(2014)0219 or the Droutsas report (7428/14); Again proposed by Austria in Commented and Revised 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 offenses or the execution of criminal penalties, and the free movement of such data, European Commission 29 June 2015, Note 10335/15, number of the Commission Document 5833/12, footnote 166, p. 54; See also 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) COM(2012)0011 C7-0025/2012-2012/001 1(COD) P7_TA(2014)01. Both resolutions have a stricter data protection regime than the final text of the adopted EU laws. Interesting question is: Was the EU parliament not stepping over its boundaries by regulating the conditions of access to data that falls outside the scope of EU law? E.g. the police access to intelligence data for national security purposes. This question falls however outside the scope of this study.

[720] A similar omission can be found in the discussion of the Data Protection Umbrella Agreement. The majority of participants were in favor of the agreement covering private-to-government and government-to-government data transfers. Most favored the idea that the agreement should apply to existing and future bilateral agreements between the EU and individual EU Member States and the US, though some acknowledged that extending the scope to existing agreements might prove difficult in practice and might only be achieved over time. Explanatory Memorandum, Annexe au document COM(2010) 252 PO/2010/3091.

[721] Commented and Revised 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

With regard to the non-incompatibility requirement in relation to GDPR-data that is being transferred from a private entity or another public authority the Commission commented that "if a legal obligation to transfer data to the police existed, such transfer would be considered as the initial police processing" under the LED.[722] The Commission underlined that if the initial "purpose was outside the scope of the Directive the GDPR was applicable" and referred to Article 6.4 GDPR.[723] For the Commission the "crucial point was that there were no gaps in the protection."[724]

In my opinion, the back and forth references between the LED and the GDPR that were made during the legislative process of the new regulatory framework turns out to be problematic for the effective protection of fundamental rights and freedoms in data-driven crime detection. In the end the GDPR and the LED reference each other in quite a general manner. The LED notes that the GDPR is applicable when data is being processed for other purposes than the ones referred to in art. 1(1) GDPR, and from the scope of the GDPR is excluded data processing by competent authorities for the purposes that pursue LED objectives. Member States can entrust competent authorities with tasks which are not necessarily carried out for the LED objectives. The processing of personal data for those purposes that pursue those other objectives, in so far as it is within the scope of EU law, falls within the scope of the GDPR.[725]

---

the purposes of prevention, investigation, detection or prosecution of criminal offenses or the execution of criminal penalties, and the free movement of such data, European Commission 29 June 2015, Note 10335/15, number of the Commission Document 5833/12, footnote 151, p. 50, 29 June 2015.

[722] Commented and Revised 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 offenses or the execution of criminal penalties, and the free movement of such data, European Commission 29 June 2015, Note 10335/15, number of the Commission Document 5833/12, footnote 151, p. 50, 29 June 2015.

[723] Commented and Revised 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 offenses or the execution of criminal penalties, and the free movement of such data, European Commission 29 June 2015, Note 10335/15, number of the Commission Document 5833/12, footnote 151, p. 50, 29 June 2015.

[724] Commented and Revised 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 offenses or the execution of criminal penalties, and the free movement of such data, European Commission 29 June 2015, Note 10335/15, number of the Commission Document 5833/12, footnote 151, p. 50, 29 June 2015.

[725] Article 9(1) and (2) LED; Article 2(2)(d) GDPR; Recital 19 GDPR: "The protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention,

By not adopting the amendment and only relying on the provisions of the GDPR, the protection level is lowered for non-voluntary data transfers compared to the protection that would have been offered if the amendment had been codified. This is due to three changes. First of all, the GDPR provisions allow for access by the authorities to private entity-held GDPR-data for all objectives of art. 1(1) LED, including detection and prevention of crime and safeguarding against and the prevention of threats to public security. Secondly, with the amendment access was only made possible in a specific case when reasonable grounds gave reason to believe that the processing of the personal data would substantially contribute to the investigation or prosecution of criminal offenses. Thirdly, art. 6(4) juncto 23(1) GDPR does not prescribe safeguards to the access to private entity-held GDPR-data by competent authorities, such as written and documented requests. The amendment did prescribe this.

5.4.2 Recital 50 GDPR for processing GDPR-data for LED purposes

This subsection contributes to the answer to the subquestion: How are voluntary data transfers of GDPR-data for LED objectives regulated in the European data protection framework? For voluntary data transfers the EU legislature enacted the last two sentences of Recital 50 of the GDPR.

Recital 50 GDPR states:

> Indicating possible criminal acts or threats to public security by the controller and transmitting the relevant personal data in individual cases or in several cases relating to the same criminal act or threats to public security to a competent authority should be regarded as being in the legitimate interest pursued by the controller. However, such transmission in the legitimate interest of the controller or further processing of personal data should be prohibited if the processing is not compatible with a legal, professional or other binding obligation of secrecy.

investigation, detection or prosecution of criminal offenses or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security and the free movement of such data, is the subject of a specific Union legal act. This Regulation should not, therefore, apply to processing activities for those purposes. However, personal data processed by public authorities under this Regulation should, when used for those purposes, be governed by a more specific Union legal act, namely Directive (EU) 2016/680 of the European Parliament and of the Council (1)".

The situation described in this recital concerns *voluntary* data sharing which also occurs without the knowledge or consent of the data subject. The transfer is therefore not based on a *lex specialis* as required in art. 6(4) juncto 23(1)(d) GDPR because that would annul the voluntariness of the transfer, nor is it based on the renewed consent ex art. 6(4) juncto art. 6(1(a) GDPR.[726] These art. 6(4) GDPR arrangements are the only two derogations that can be made to the rule of cumulation of the four data protection touchstones.[727]

In the case of Recital 50 the legislature proposes the so-called *f-ground*[728] for voluntary data transfers from private entities to criminal law enforcement authorities. The *f-ground* prescribes that the processing is lawful when it is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data.[729]

Because art. 6(1)(f) GDPR is not included as an derogation in art. 6(4) GDPR, the non-incompatibility requirement applies and cannot be overruled by this new processing ground. This means that the processing that is described in Recital 50 can only be lawful when it is compatible with the initial processing purposes. Also, when it comes to voluntary disclosures no legal obligation is underlying the transfer, and the competent authority to whom the data is disclosed cannot qualify as a receiver and should instead be considered a recipient of the personal data. For these transfers the GDPR demands transparency as described in Section 4.1.1.2.

The purpose of potentially sharing of personal data with criminal law enforcement authorities must be specific and legitimate and be made explicit prior to the data collection. Frequently these purposes are mentioned in the privacy statements of private entities. For example, Booking.com states: “We disclose personal data to law enforcement insofar as it [...] is strictly necessary for the prevention, detection or prosecution of criminal acts and fraud or if we are otherwise legally obliged to do so [...].”[730] Facebook explains in its privacy policy: “We [...] share your information

[726] See Section 5.3.

[727] The rule of cumulating touchstones was described in Section 3.5 on page 79: a processing ground cannot substitute for the non-incompatibility requirement because these are cumulating data protection touchstones.

[728] This ground owes his name to its placement in the GDPR and preveiously in the DPD: art. 6(1)(f) GDPR.

[729] Article 6(1)(f) GDPR.

[730] See privacy statement Booking.com https://www.booking.com/content/privacy.en-gb.html Version:

with law enforcement when we have a good-faith belief that it is necessary to detect, prevent and address [...] illegal activity."[731] Whereas Booking.com limits the potential sharing of data with competent authorities to instances that are strictly necessary, Facebook does not. As described on page 68 the EDPB have warned against elastic purposes in the past and listed "law enforcement" as being not specific enough. The question is whether the purpose "detect, prevent and address illegal activity" is not just as vague as the purpose "law enforcement".

Recital 50 limits the use of the processing ground art. 6(1)(f) GDPR to transfers that concern data indicating possible criminal acts or threats to public security. The personal data must also be relating to individual cases or several individual cases. This means that the personal data must be directly relating to one or more natural persons. Data transfers that concern bulk data fall outside the scope of Recital 50 when this data that is transferred in relation to crime.[732]

A strong statement like this, cannot be made for data that is transferred because it matches a general profile. In principle data that matches a general profile can be indicative of possible criminal acts and therefore could fall under the scope of Recital 50. However, the recital also speaks of cases relating to the same criminal act, which indicates that a concrete criminal offense must be detected and not a statistical likelihood. How this recital must be interpreted in light of profiling and predictive policing is yet to be determined in the case law.[733]

Because of the underlining of the *individual cases or several cases relating to the same criminal act* Recital 50 GDPR also only covers *ad hoc* data transfers in which the data is handed-over. It does not facilitate structural partnerships where the competent authority is granted direct access to the database of the private entity.

Article 6(1)(f) GDPR cannot provide a lawful processing ground where the data transfer is not compatible with a legal, professional or other binding obligation of

2019-12-22 15:40:14. Lastly retrieved 22 December 2019.

[731] See privacy statement facebook.com https://en-gb.facebook.com/about/privacy#legal-requests-prevent-harm. Date of last revision: 19 April 2018; Lastly retrieved 22 December 2019.

[732] This might be different for date relating to several cases relating to public security. See Recital 50 GDPR. Data transfers for this purpose fall outside the scope of this study. yet, the text of the Recital seems to imply that the data still has to relate to *cases* excluding the transfer of bulk data which includes personal data of individuals that have no connection to the cases relating to public security.

[733] Looking forward to initiate steps toward strategic litigation on these points with human rights organizations.

secrecy. Professional obligations for secrecy include, amongst others, the attorney-client-, doctor-patient-, and clergy-penitent privilege, contractual obligations for secrecy can, for example, refer to non-disclosure agreements, and legal obligations of secrecy include a wide variety of obligations of which the confidentiality provisions of the ePrivacy Regulation are most relevant in this study.[734] That Regulation safeguards that electronic communications and their metadata should be kept confidential by providers of electronic communications networks and -services.[735] For the purposes of criminal law enforcement or public security, it is only permitted to derogate from this rule when the restriction is provided by law or on the base of consent of the data subject.[736] The breach of confidentiality that would occur from voluntary personal data transfers from providers of electronic communications networks and -services to competent authorities can, therefore, not lawfully be based on the art. 6(1)(f) GDPR ground and instead should be based on a derogation of the non-incompatibility requirement: a *lex specialis* ex art. 6(4) juncto art. 6(1)(c) GDPR.

Pursuant to the art. 6(1)(f) GDPR ground a balancing test should be made between the legitimate interests of the data controller and the interests for fundamental rights protection of the data subject. The legitimate interests of a controller, including those of a controller to whom the personal data may be disclosed, or of a third party, may provide a legal basis for processing, provided that the interests or the fundamental rights and freedoms of the data subject are not overriding.[737] The factors of that

[734] The ePrivacy Regulation has not yet been adopted when I submitted this study. See http://www.europarl.europa.eu/legislative-train/theme-connected-digital-single-market/file-jd-e-privacy-reform. Lastly retrieved 22 December 2019.

[735] Any interference with electronic communications is prohibited. Providers of electronic communications networks and services are prohibited to process the electronic communications data for other purposes than the purpose of transmission of the communication. Metadata can be processed for a wider set of technical and billing purposes on the base of the ePrivacy Regulation or on the base of consent. Current version: Committee report tabled for plenary, 1st reading/single reading, Draft European Parliament Legislative Resolution on the proposal for a regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications, Amendment 68 amending art. 5 ePrivacy Regulation and Amendment 71 amending art. 6(1) ePrivacy Regulation).

[736] Current version: Committee report tabled for plenary, 1st reading/single reading, Draft European Parliament Legislative Resolution on the proposal for a regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications, Amendment 121 amending art. 11b(new) ePrivacy Regulation).

[737] Recital 47 GDPR.

test include:[738]

- the nature and source of the legitimate interest and whether the data processing is necessary for the exercise of a fundamental right, is otherwise in the public interest, or benefits from recognition in the community concerned;
- the impact on the data subject and their reasonable expectations about what will happen to their data, as well as the nature of the data and how they are processed;
- additional safeguards which could limit undue impact on the data subject, such as data minimization, privacy-enhancing technologies; increased transparency, general and an unconditional right to opt-out, and data portability.

The legitimate interest described in Recital 50 GDPR is the indication of possible criminal acts or threats to public security by the controller and transmission of the relevant personal data in individual cases or in several cases relating to the same criminal act or threats to public security to a competent authority. As discussed in Section 5.1.3 on page 145, the transfer of personal data to competent authorities for LED purposes is considered an interference with the rights protected in art. 8 ECHR and art. 7 CFREU. The outcome of this balancing test is dependent on many variables that depend on the circumstances of the case.

5.4.3 A critical note on Recital 50 GDPR

An important subquestion concerns to what extent the purposes of processing of the private entity can affect the lawfulness of the data collection by the criminal law enforcement authority when this data is voluntarily transferred by the private entity. The way in which Recital 50 GDPR attempts to deal with this, is unsatisfactory on multiple grounds.

First of all, with the stressing of these criminal law enforcement interests as interests of the data controller, data controllers might be tempted to process personal data for these extra purposes for future unknown but criminal law enforcement related reasons. Recital 50 GDPR also has the potential of stimulating competent authorities to

[738] Article 29 Working Party *Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC*, 2014, WP 217, p. 3.

approach data controllers to convince them to process data for the purposes of Recital 50 GDPR and keep the data available for criminal law enforcement purposes. The Europol Regulation prohibits active procurement with private entities, but the LED is silent on this matter.[739] The Recital can easily fall prey to mission creep, which was described on page 77, something that might lead to a culture where competent authorities request data from data controllers on a voluntary base ex art. 6(1)(f) GDPR before or in stead of using the legislative measures for search and seizure of data on the base of which the data controller is obligated to transfer the data ex art. 6(1)(c) GDPR. This turn of events would lead to a systematic decline of safeguards for the protection of fundamental rights and freedoms of the data subject.

Secondly, in my eyes the data controller is badly equipped to balance interests of fundamental rights protection and interest that involve the detection, prevention, investigation ad prosecution of criminal offenses. What is more, with the rejection of the amendment, the legitimacy of access by competent authorities to data held by private entities is not specifically regulated. The competent authorities can accept voluntary transfers of data by private entities that would not pass the balancing test of art. 6(1)(f) GDPR, without consequences for the legitimacy of the further processing by the competent authorities. Is this Recital not accidentally making a loophole that encourages private entities to process data in violation with fundamental right protection?

The last issue that arises is the question of initial processing and further processing under the LED. With regard to the non-incompatibility requirement in relation to GDPR and data transfers from a private entity or another public authority to competent authorities, the Commission stated that where a legal obligation to transfer data to the police existed, such transfer would have to be considered as the initial police processing under the LED. In the case of data transfers based on Recital 50 juncto art. 6(1)(f) GDPR no legal obligation to transfer data to the police exists. The question is whether the act of receiving the data should be considered initial police processing or further police processing, and what this qualification entails for the protection of fundamental rights and freedoms of the data subject. The next Section will

[739] Under the Europol Regulation the agency is explicitly not allowed to process information that has clearly been obtained in obvious violation of human rights. Article 23(9) Europol Regulation. There is also an explicit prohibition for Europol to contact private entities or persons to disclose data. Article 26(9) and art. 27(4) Europol Regulation.

discuss these matters.

5.5 Re-use of LED-data for LED purposes

This section investigates the next type of use limitation in order to gain full understanding of the types of use limitation in European data protection law and their relationship with the purpose limitation principle. This section also investigates to what extent further use of personal data lead to an infringement of fundamental rights and in what way is the non-incompatibility requirement connected to the justification criteria for fundamental rights infringements?

The non-incompatibility requirement is secured in the LED, which has been described in Section 5.1. The European data protection framework knows several derogation clauses to this rule of compatibility that allow re-use of personal data for incompatible purposes. Under the GDPR re-use is only lawful when the data subject either consented to the new processing purposes[740] or when the re-use is based on a *lex specialis* as required in art. 6(4)GDPR which includes the justification criteria of fundamental rights law.[741] A derogation clause based on similar criteria as the latter GDPR derogation is also included in the LED: art. 4(2) LED.

This Section discusses the case law of the ECtHR that concerns re-use for incompatible purposes that would fall under the scope of the LED. The outcome of this case law study will be discussed in light of the criteria that have been laid down by art. 4(2) LED. That provision allows re-use of personal data when the new processing purposes fall under the scope of the LED and the processing meets the justification criteria stemming from fundamental rights law. The conclusion of this discussion will be used, firstly, to understand use limitation in the field of criminal law enforcement and public security, and secondly, to assess the value of the non-incompatibility requirement for data processing under the scope of the LED.

5.5.1 Problematic phrasing of art. 4(2) LED

In Section 1.2 on page 10 of this study I made a difference in terminology for purposes that refer to the explicit specific and legitimate processing purposes and purposes that

[740] See Section 5.3 on page 171 for the discussion of consent in relation to re-use of personal data.
[741] See Section 5.2 on page 151 to this extent.

refer to the scope of the LED. The former are called *purposes* in this study and the latter *LED objectives* or *criminal law enforcement and public security objectives*. The EU legislature has not made this distinction in vocabulary. Which is unfortunate, specifically for the clarity of the rules on re-use under the LED ex art. 4(2). That provision would have benefitted from a more precise wording in general. In the following paragraphs I point to the ambiguity of art. 4(2) LED and guide the reader in the direction of – what is in my opinion – the correct interpretation. Article 4(2) LED states the following:

> Processing by the same or another controller for any of the purposes set out in Article 1(1) other than that for which the personal data are collected shall be permitted in so far as:
>
> a the controller is authorised to process such personal data for such a purpose in accordance with Union or Member State law; and
>
> b processing is necessary and proportionate to that other purpose in accordance with Union or Member State law.

The first problem arises in the first half of the first sentence. The legislature refers to *the purposes set out in art. 1(1) LED*, which are the prevention, investigation, detection or prosecution of criminal offenses or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security. As discussed in Section 4.1 of this study processing purposes have to be specific enough for the data controller to make constructive decisions with regard to, for example, data minimization and storage limitation.[742] The objectives set out in art. 1(1) LED are too vague to serve as processing purposes in the sense of art. 4(1)(b) LED, because a purposes like the *investigation of crime* would justify all types of data to be stored for long periods because it might come in handy in a future investigation. Article 4(2) LED would have been more on point with the purpose specification requirement if it, instead of *[...] the purposes set out in Article 1(1) [...]*, would have stated: *[...]a purpose in pursuance of any of the objectives set out in Article 1(1) [...]*.

The second problem arrises in the second half of the first sentence, which speaks of *purposes other than that for which the personal data are collected*. This text could

[742] See Section 4.1.3.4 on page 106 on this topic.

be interpreted as at odds with the non-incompatibility requirement, which is applicable to all data processing under the LED pursuant to art. 4(1)(b) LED. The non-incompatibility requirement lays down the rule that personal data can be lawfully further processed for other purposes than those for which the personal data is collected, as long as those other purposes are compatible with the initial purposes.[743] Article 4(2) LED would have been more in-line with the non-incompatibility requirement if, instead of *[...] other than that for which the personal data are collected [...]*, it would have stated: *[...] which is incompatible with the purposes for which the personal data are collected [...]*.

When combined, the above clarifications help in understanding the two subparagraphs of art. 4(2) LED:

> *Processing by the same or another controller for a purpose in pursuance of any of the objectives set out in Article 1(1) which is incompatible with the purposes for which the personal data are collected shall be permitted in so far as:*
>
> a. *the controller is authorized to process such personal data for such a purpose in accordance with Union or Member State law; and*
> b. *processing is necessary and proportionate to that other purpose in accordance with Union or Member State law.*

In the following subsections I will discuss art. 4(2) LED based on this interpretation.

5.5.2 Re-use criteria of art. 4(2) LED repeat already existing obligations

Similar to art. 6(4) juncto art. 23(1) GDPR,[744] art. 4(2) LED connects the lawfulness of re-use to the justification criteria that are well known from fundamental rights law. The first sentence of art. 4(2) LED describes the legitimate aim,[745] the first subparagraph encapsulates the legality criterion,[746] and the second subparagraph puts

[743] Section 5.1.1.3 on page 135 described the applicability of the factors of the compatibility test to further use under the LED.

[744] Re-use based on these provisions is has been discussed in Section 5.2.

[745] See Section 5.2.2.3.1 on page 160.

[746] See Section 5.2.2.3.2 on page 162.

forward the necessity criterion.[747] Despite these similarities, the effect of art. 4(2) LED on the limitation of data processing is in my opinion very different from the effect of art. 6(4) GDPR. Not all re-use of GDPR-data for GDPR purposes constitutes a fundamental rights infringement. Yet, when the data controller is not in the position to lawfully obtain consent from the data subject but nevertheless plans on re-using the data, art. 6(4) GDPR obligates her to apply the justification criteria stemming from fundamental rights law. The application of the fundamental rights criteria limit the processing of personal data because only a small subset of intended re-use can be justified in terms of fundamental rights law. For example, not all data controllers can move the legislature to enact a legislative measure that would justify the intended re-use for the new purposes.

In contrast, almost all re-use of LED-data constitutes a fundamental rights infringement, not because the data is being re-used but because the data is processed by a competent authority for LED objectives. The case law of the ECtHR demonstrates that in the field of criminal law enforcement and public security data collection and storing is frequently enough to amount to an interference with the rights protected under art. 8(1) ECHR and the actual secondary use is not decisive for the applicability of art. 8(2) ECHR.[748] In the *Kopp*-case, for example, the government contended that the question whether there had been interference by the authorities with the applicant's private life and correspondence remained open, since none of his telephone conversations that were recorded by the police had been brought to the knowledge of the prosecuting authorities. All the recordings had been destroyed and no use whatsoever had been made of any of them.[749] Similar arguments were made in the *Amann*-case, when the government argued that the applicant had not in any way been inconvenienced as a result of the creation and storing of a card on the applicant for the security card index, and that the card in all probability had never been consulted by a third party.[750] In both cases the ECtHR rejected the assertions and explained that the subsequent use of the data has no bearing on the finding that the storing or recording of information relating to an individual's private life by a public

[747] See Section 5.2.2.3.3 on page 167.

[748] See for example ECtHR 17 December 2009, no. 16428/05 (*Gardel/France*), par. 58.

[749] ECtHR 25 March 1998, no. 23224/94 (*Kopp/Switzerland*), par. 51.

[750] ECtHR 16 February 2000, no. 27798/95 (*Amann/Switzerland*), par. 68; This reasoning can also be found in ECtHR 4 December 2008, no.130562/04 and 30566/04 (*S. and Marper/the United Kingdom*).

authority amounts to an interference within the meaning of Article 8.[751] In the *S. and Marper*-case, the ECtHR noted that the applicants' fingerprints were initially taken in criminal proceedings and subsequently recorded in a national database with the aim of being permanently kept and regularly processed by automated means for criminal-identification purposes and for the purpose of increasing the size and utility of the database in order to train algorithms.[752] During the discussion of the applicability of art. 8(1) ECHR, the ECtHR was silent on this change in processing purpose and instead focussed on the nature of information contained in fingerprints and the effects of storing this information.[753] When testing the legitimacy of the interference under art. 8(2) ECHR the ECtHR explained that the secondary processing purposes lacked a pressing social need and were, therefore, not necessary in a democratic society.[754] The legitimacy, necessity and proportionality of the new processing purposes were central to the ECtHR's assessment because the data was being processed by competent authorities for LED objectives, the fact that the processing purpose changed did not aggravate the ECtHR.[755]

This means that almost all data processing by competent authorities for a purpose in pursuance of the LED objectives must meet the strict art. 8(2) ECHR criteria, regardless of that being for initial, new compatible, or new incompatible purposes. So other than a moment to pause and reflect on the intended re-use, the criteria of art. 4(2) LED provide no additional burden to the re-use of personal data because the obligation to apply the fundamental rights criteria was already prescribed by the fundamental rights framework itself.

What is more, the criteria that are put forward in art. 4(2) LED echo those of art. 4(1) LED, which is applicable to all data processing regardless of that being for initial, new compatible or new incompatible purposes. The safeguard of art. 4(2)(a) LED is similar to the principle of lawful processing ex art 4(1)(a) LED, which should

[751] ECtHR 25 March 1998, no. 23224/94 (*Kopp/Switzerland*), par. 53; ECtHR 16 February 2000, no. 27798/95 (*Amann/Switzerland*), par. 69; ECtHR 17 December 2009, no.16428/05 (*Gardel/France*), par. 58.

[752] ECtHR 4 December 2008, no.130562/04 and 30566/04 (*S. and Marper/the United Kingdom*).

[753] ECtHR 4 December 2008, no.130562/04 and 30566/04 (*S. and Marper/the United Kingdom*), par. 86.

[754] ECtHR 4 December 2008, no.130562/04 and 30566/04 (*S. and Marper/the United Kingdom*), par. 123-125.

[755] See also Section 5.1.3.1 on the link between purposes and foreseeability in relation to further use under the GDPR.

be taken into account together with the one single processing ground that is presented for the field of criminal law enforcement and public security: art. 8 LED which requires that the data processing is "necessary for the performance of a task carried out by a competent authority for the purposes set out in Article 1(1) and that it is based on Union or Member State law." The safeguard of art. 4(2)(b) LED demands that the secondary processing is necessary and proportionate to that other purpose in accordance with Union and Member State law. The EDPB connected the fundamental rights criteria of necessity and proportionality to the data protection principles in their Opinion on the Application of Necessity and Proportionality Concepts and Data Protection within the Law Enforcement Sector, in particular lawfulness and fairness, purpose specification, data minimization and storage imitation.[756] These data protection principles are codified in art. 4(1)(a), (b), (c) and (e) LED. This means that the fundamental rights criteria have already been implemented in the data protection principles to a large extent and art. 4(2) is not adding additional criteria or safeguards that have to be met to justify the re-use of personal data.[757]

5.5.3 Article 4(2) LED and the international law obligations of the EU Member States

As described in Section 2.2.1.1 the DPC is signed by all EU Member States and applies to all fields of data processing, including the field of criminal law enforcement and public security. The DPC ensures that derogations on the non-incompatibility requirement must be justified in terms of legitimate aim, legality, necessity and pro-

[756] Article 29 Working Party *Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector*, 2014, WP 221.

[757] We see a similar *empty* safeguard in the Europol Regulation. Recital 25 of the Europol Regulation states 'Europol should ensure that all personal data processed for operational analyses are allocated a specific purpose. Nonetheless, in order for Europol to fulfill its mission, it should be allowed to process all personal data received to identify links between multiple crime areas and investigations, and should not be limited to identifying connections only within one crime area.' This is detailed in art. 18(3)(b) Europol Regulation: When data can be useful for the purpose for other operational analysis projects than the one for which the data was collected, the further processing should firstly meet the criteria of necessity and proportionality, and secondly, the Executive Director has to define the specific purpose, categories of personal data and categories of data subjects, participants, duration of storage and conditions for access, transfer and use of the data concerned, and must inform the Management Board and the EDPS thereof. These two safeguards also apply to processing for the initial purposes, ands do not add additional safeguards.

portionality, and must respect the essence of fundamental rights.[758] By incorporating these criteria in art. 4(2) LED Member States experience no inconsistencies in their obligations under supranational- and international data protection law. The criterion in *respect for the essence of the right* applies automatically to all data processing that falls under the scope of EU law.[759]

5.5.4 Default use limitation ex art. 4(2) LED

Because art. 4(2) LED repeats criteria that already exist in other obligations, article 4(2) LED does not pose additional limitations to the re-use of personal data in the way that art. 6(4) juncto 23(1) GDPR does. It will be common-practice for the competent authority to already meet the criteria of this derogation to the non-incompatibility requirement. This results, in my eyes, to a much smaller role of the non-incompatibility requirement under the LED, than under the GDPR. The limitations that the non-incompatibility requirement puts on the processing of personal data, will frequently be overturned by this re-use derogation that allows re-use of personal data for incompatible purposes. The competence that art. 4(2) LED refers to is in the field of the criminal law enforcement frequently articulated as an objective rather than a competence in relation to a specific purpose. The existence of these broad competences accelerates the re-use of personal data for incompatible purposes.

So in my eyes art. 4(2) LED is the exception that becomes the rule in practice.

[758] derogating measures must be provided for by law, respects the essence of the fundamental rights and freedoms and constitute a necessary and proportionate measure in a democratic society for a specific legitimate aim, which includes the investigation and prosecution of criminal offenses, national security and public safety. art. 11(1)(a) DPC and art. 5(4)(b) DPC. In this provision the detection of crime, under which the pre-crime phase of this study falls, is not mentioned in the same breath as the prevention, investigation and prosecution of criminal offenses. The detection can nevertheless in my opinion be categorized under the prevention of criminal offenses and qualifies as an essential objective of general public interest; Article 11 shows the interplay between the jurisdiction of the CoE and EU. The doctrine of the *essence of the right* stems from the CFREU, a legal instrument of the EU, and is now transcribed in the DPC, a CoE international treaty.

[759] See Section 2.1.2.1 on the scope of the CFREU that follows the scope of EU law. Peculiarly enough, the EU legislature did feel the need to underline respect for the essence of rights when restrictions are made on the data protection principles, rights and obligations pursuant to art. 23 GDPR. To my opinion this was not necessary in terms of protection for the reasons that are discussed in the main text. See also Section 5.2.2.2 where the safeguards of 6(4) GDPR are compared to those of art. 23 GDPR and a similar point is made.

According to settled case law of the CJEU and ECtHR restrictions on fundamental rights and freedoms must be interpreted restrictively and exemptions from general rules must be applied only in specific and limited circumstances.[760] When looking at the conclusions of the previous subsection, the question is whether this restrictive interpretation also should be applied to derogations on the non-incompatibility requirement in the field of criminal law enforcement and public security because neither the CJEU nor the ECtHR has identified re-use of personal data within the field of criminal law enforcement and public security as an interference with fundamental rights.[761]

The default of use limitation based on art. 4(2) LED is visible in the text of the LED too. This re-use rule is positioned in art. 4 LED named *Principles relating to the processing of personal data* as an independent rule with its own weight next to the traditional data protection principles presented in art. 4(1) LED.[762] Also, the preamble of the LED already explains use limitation in light of the possibility to process personal data for new incompatible purposes that pursue the objectives of the LED. Recital 29 lays down that "personal data should be collected for specified, explicit and legitimate purposes within the scope of this Directive and should not be processed for purposes incompatible with the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security".[763] For this reason I argue that art. 4(2) LED changes the default limitation from compatibility between purposes to justifiability of the new purposes under the criteria stemming from fundamental rights law.

Nevertheless, I do see an added value in art. 4(2) LED, because the enforcement of art. 4(2) LED has the potential to accelerate the securing of fundamental rights cri-

[760] ECtHR 23 February 2016, no. 40378/06 (*Y.Y./Russia*), par. 55-56; ECtHR 15 April 2014, no. 50073/07 (*Radu/the Republic of Moldova*), par. 28-31; CJEU 21 December 2016, C-203/15 and C-698/15 (*Tele2 Sverige/Post-och telestyrelsen* and *Secretary of State for the Home Department/Tom Watson, Peter Brice, Geoffrey Lewis*).

[761] See Section 5.1.2.2 for an analysis of the case law of the CJEU and incompatible re-use of personal data; Also, the Council of Europe gave guidance as to the interpretation of derogations on the non-incompatibility requirement in the police sector, as discussed in Section 2.2.1.2 on page 48. The Council of Europe recommended that personal data collected and stored by the police for police purposes should be used exclusively for those purposes. These recommendations date as far back as 1987.

[762] See Section 2.2.1.1 on 47.

[763] Recital 29 LED.

teria in the day-to-day protocols of competent authorities. Article 41 LED lays down the obligation for Member States to provide for an independent supervisory authority to monitor the application of the LED. This authority must also enforce the correct application of art. 4 LED. Because of the overlapping criteria in the LED and in fundamental rights law, so in a sense the supervisory authority also oversees the justifiability of privacy infringements. This is good news for the protection of fundamental rights, because the enforcement procedures of the supervisory authorities have the potential to be much faster and hands-on than a procedure at the CJEU or ECtHR. The combination of independent oversight and the embedding of the justification criteria in the LED can lead to standard fundamental rights compliance in the data processing protocols of competent authorities.

5.6 Re-use based on privileged purposes

This section further researches the role of the non-incompatibility requirement is data protection law, it investigates other types of use limitation and researches the relationship between the purpose limitation principle and these other types of use limitation. The further processing of personal data for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes is considered processing for privileged purposes under European data protection law.[764] In the following subsection I will briefly discuss this type of re-use of data. See Section 4.1.5.5 for a discussion of the purpose specification requirement and privileged purposes.

5.6.1 Further processing for the good of knowledge increase

Privileged purposes are connected to the idea of a knowledge society and the legitimate expectations of society for an increase of information.[765] The privileged purposes can serve a wide variety of interests, for example the public interest that is served with health research and the commercial interests that are being served with

[764] [Forgó et al., 2017, p. 36].

[765] The GDPR specifically mentions the goal of knowledge increase in light of data transfers to third countries in Recital 113 GDPR. The GDPR fails to mention, however, which expectations should be taken into account in that context: the knowledge increase in the society of the third country or the knowledge increase in the transmitting EU Member State?

statistical market research. Whether further processing of data for these purposes passes the compatibility test, depends on the compatibility between the initial purposes and new purposes. For the majority of processing operations this is not likely to be the case. So in order to single out processing for these privileged purposes from processing for other new incompatible purposes the EU legislature had to be creative. In the GDPR further processing for archiving purposes in the public interest, scientific and historical research purposes, and statistical purposes is considered to be a compatible lawful processing operation that does not interfere with the requirement of non-incompatibility.[766] For the LED the legislature did not have to be as resourceful. As described in Section 5.5 of this study, art. 4(2) LED foresees in the re-use of personal data when processing for the new purposes pursues the LED objectives and meets the justification criteria stemming from fundamental rights law. Some processing for privileged purposes will meet the criteria of art. 4(2) LED. All other processing for privileged purposes that pursues other objectives falls under the scope of the GDPR ex art. 4(3) LED.[767]

Following the LED and the GDPR the specific rules are not intended as a general authorization to further process data in all cases for historical, statistical or scientific research.[768] Processing for these privileged purposes is only lawful where appropriate safeguards for the rights and freedoms of data subjects are met.[769] Even though the privileged purposes fall under this special arrangement when it comes to the non-compatibility requirement, the other component of the purpose limitation principle, the purpose specification requirement, remains intact. The purposes still have to be legitimate, explicit and specified.[770] What is more, according to the EDPB privileged purposes should be interpreted strictly.[771] A generic reference to research, for exam-

[766] Second sentence art. 5(1)(b) GDPR juncto Recital 50 GDPR.For Europol a similar strategy is chosen, with the exception that archiving purposes are excluded from the privileged purposes in the Europol Regulation. Art. 28(1)(b) Europol Regulation

[767] Article 9(2) LED directs to the GDPR for this type of processing: Where competent authorities are entrusted by Member State law with the performance of tasks other than those performed for the purposes set out in Article 1(1), Regulation (EU) 2016/679 shall apply to processing for such purposes, including for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, unless the processing is carried out in an activity which falls outside the scope of Union law.

[768] Article 29 Working Party *Opinion on Purpose Limitation*, 2013, WP 203, p. 28.

[769] Article 4(3) LED; and art. 5(1)(b) juncto 89 GDPR.

[770] See Section 3.3 on page 61 of this study on the different elements of the purpose limitation principle and their relationship to the two components.

[771] Strict interpretation of the purposes has consequences for data processing in big data set-

ple, is not good enough.[772] Similarly, the processing of personal data for statistical purposes cannot include processing that is aimed at taking measures against an individual data subject.[773] Statistical purposes imply that the result of processing is not personal data, but aggregated data, and that this result or the personal data are not used in support of measures or decisions regarding any particular natural person.[774] In the following subsections I discuss the characteristics of further processing for these privileged purposes under the GDPR.

5.6.2 The influence of the DPC on art. 5(1)(b) GDPR

Further processing for privileged purposes is exempted from the cumulation rule for the non-incompatibility requirement in the second sentence of art. 5(1)(b) GDPR.[775] The provision lays down that *further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes.* This proclamation of compatibility with the initial purposes feels manufactured, but is necessary for compliance with the international law obligations of the Member States that are signatory states to the DPC.[776] Under the DPC the only restrictions that are permitted for the knowledge cause are restrictions on the data subject rights and alleviations on transparency obligations for the data controller.[777] The DPC does not allow derogations from the non-incompatibility requirement for reasons of archiving in the public interest, scientific or historical research purposes or statistical purposes. By declaring further processing for privileged purposes not to be incompatible with

ups. See to this extent [Mayer-Schonberger and Padova, 2015], [Zarsky, 2016], [Forgó et al., 2017] and [Stalla-Bourdillon and Knight, 2018].

[772] Article 29 Working Party *Guidelines on consent under Regulation 2016/679*, 2018. WP 259, p. 27; See also [Stalla-Bourdillon and Knight, 2018, p. 36-37].

[773] Article 29 Working Party *Opinion on Purpose Limitation*, 2013, WP 203, p. 28.

[774] [Mayer-Schonberger and Padova, 2015, p. 326-327]; Recital 162 GDPR

[775] See Section 2.2.2.1 on page 49 of this study.

[776] See Section 2.2.1.1 on page 47 of this study. The Europol Regulation contains a similar provision. It is likely that the EU legislature anticipated on the accession of the EU to the ECHR and considered the DPC as containing the rules as to how to process data relating to private life that also qualifies as personal data.

[777] Article 8 and 9 juncto art. 11(2) DPC; The further processing for privileged purposes should also be subject to appropriate safeguards and provided by law and must show no recognisable risk of infringement on the rights and fundamental freedoms of data subjects ex art. 8 and 9 juncto art. 11(2) DPC; art. 5(b) DPC.

the initial purposes, the EU legislature averted potential conflicts with this treaty obligation for the Member States.

5.6.3 Safeguards and the privileged purposes

Under the GDPR processing of personal data for privileged purposes must be based on one of the legal grounds of art. 6(1) GDPR.[778] Article 89 GDPR helps to assess under what conditions further use may be legal but art. 5(1)(b) juncto art. 89 GDPR cannot provide a substitute for an appropriate lawful ground for the processing because the general rule of cumulating data protection touchstones is still applicable.[779]

Further processing for privileged purposes is no acquittal for accountability of the data controller, proportionality of the data processing, or the application of other data protection principles, such as data minimization and storage limitation.[780] With the coming into force of the GDPR the criteria for these safeguards are enclosed in art. 89 GDPR. The Member States are still responsible for the safeguards to be taken for processing for privileged purposes under the LED.[781] The safeguards that the data controller implements need to be strong enough to exclude – or at least minimize – any risks to rights and freedoms of the data subjects.[782] All relevant circumstances and factors must be taken into account when deciding what safeguards, if any, can be considered appropriate and sufficient.[783]

[778] See Section 3.5.2; Article 29 Working Party *Opinion on Purpose Limitation*, 2013, WP 203, p. 33.

[779] See Section 3.5 on page 79 of this study; Article 29 Working Party *Opinion on Purpose Limitation*, 2013, WP 203, p. 33.

[780] The data processing has to meet the criterion of proportionality: if the objectives can be attained by processing anonymous information the processing of personal data is prohibited. CJEU 16 December 2008, C-524/06, (*Huber/Germany*) par. 65; Article 29 Working Party *Opinion on Purpose Limitation*, 2013, WP 203, p. 28-29; See also EDPS, 23 January 2019, *Opinion 3/2019 concerning the Questions and Answers on the interplay between the Clinical Trials Regulation (CTR) and the General Data Protection regulation (GDPR) (art. 70.1.b))*.; Under the DPD the EU Member States were obligated to provide appropriate safeguards for processing for privileged purposes, but the DPD did not provide guidance as to what safeguards would be appropriate. See Article 29 Working Party *Opinion on Purpose Limitation*, 2013, WP 203, p. 28.

[781] Article 4(3) LED.

[782] Article 29 Working Party *Opinion on Purpose Limitation*, 2013, WP 203, p. 28-29.

[783] Article 29 Working Party *Opinion on Purpose Limitation*, 2013, WP 203, p. 28. See also EDPS, 23 January 2019, *Opinion 3/2019 concerning the Questions and Answers on the interplay between the Clinical Trials Regulation (CTR) and the General Data Protection regulation (GDPR) (art. 70.1.b))*.

5.7 Stringent purpose limitation

This section discusses the last type of use limitation that exists next to use limitation based on compatibility of purposes in European data protection law. This section also contributes to answering the question what the role of the purpose specification requirement is in cases of data processing that is limited by this type of use limitation.

In a few instances the European data protection framework lays down the explicit purpose specification and attaches to this specification the obligation to process the data for this exact purpose. In those cases use limitation is based on stringent interpretations of the prescribed explicit purpose specification that is stipulated by the law or by the data controller.

5.7.1 Identification of the data subject

Data controllers who have reasonable doubts concerning the identity of the natural person making an access-, rectification-, erasure-, or restriction request ex art. 14 and 16 LED or art. 15 to 21 GDPR, have the possibility to request additional information necessary to confirm the identity of the data subject.[784] The Recital of the LED explains that this additional personal data may be processed only for the specific purpose of identification and should not be stored for longer than needed for that purpose.[785] The purposes of processing are stipulated in the LED, namely the identification of a natural person that makes a data subject request, and the use limitation on this processing operation is based on a stringent interpretation of this prescribed explicit purpose specification. The data that the data controller learns in this identification process cannot be processed for any other purpose, including processing for privileged purposes. The GDPR lacks any emphasis on the further use of the identification data, and therefore it is likely that the use is limited based on the non-incompatibility requirement. This different type of use limitation with regard to identification data can be explained in light of the Rule of Law and the impact that further processing of identification data by competent authorities can have on rights and freedoms of the natural person concerned. This type of use limitation is

[784] Article 12(5) LED and art. 11(2) GDPR. See footnote [434] on page 104 on the implications of art. 11 GDPR with regard to the identification of the data subject.

[785] Recital 41 LED.

predominantly connected with the function of purpose limitation as safeguard in the protection of rights and freedoms of the data subject.

5.7.2 Transfers to third countries

In the field of criminal law enforcement and public security specific rules have been laid down in Chapter V of the LED for the transfers of personal data to competent authorities in third countries or international organizations. Data can be transferred when there are appropriate safeguards that surround a data transfer.[786] Recital 71 LED explains that the "controller should be able to [...] take into account the fact that the transfer of personal data will be subject to confidentiality obligations and the principle of specificity, ensuring that the data will not be processed for other purposes than for the purposes of the transfer." This concept *the principle of specificity* has not been used by the EU legislature before and appears to be stricter than purpose limitation based on compatibility of purposes, because the Recital speaks of *other* purposes. This Recital only includes processing for the purposes of the transfer and, therefore, excludes processing for compatible – but other – purposes. This type of use limitation is therefore based on stringent interpretations of purposes that have been stipulated by the data controller.

5.8 Conclusion on use limitation

The non-incompatibility requirement is fleshed out in the compatibility assessment between the initial and new purposes of processing. This test includes an assessment of the link between the purposes, context of processing, nature of the data, possible consequences of the processing on the rights and freedoms of the data subject and safeguards to mitigate the potential negative consequences. The ECtHR has based its reasoning for the establishment and impact of infringements of art. 8(1) ECHR by further use of personal data on the factors of the compatibility assessment, but not on the non-incompatibility criterion itself. A similar conclusion can be made for the CJEU, that in the estimation of EU law and fundamental rights in cases that concerned further processing of personal data systematically omitted reference to the

[786] Article 37(1)(b) LED.

non-incompatibility requirement in its reasoning for the establishment and impact of infringements of art. 7 and 8 CFREU, and instead, referred to various other data protection principles. Both courts have, however, referred to the requirement in the assessment of safeguards that mitigated the negative effects of data processing that the courts connected to restrictions on the fundamental rights.

The derogation clauses for the non-incompatibility requirement implement the triple test of art. 8(2) ECHR and its equivalent in art. 52(1) CFREU. Collection of personal data by criminal law enforcement authorities is in most cases regarded as an interference with the rights protected under art. 8 ECHR and art. 7 and 8 CFREU by the Courts. The data collection must, therefore, pass the triple test of art. 8(2) ECHR and its equivalent in art. 52(1) CFREU. The derogation clauses of the non-incompatibility requirement include these criteria that stem from fundamental rights law. The implication of this is that further use in the field of criminal law enforcement and public security is not subject to additional requirements. The default limitation on data processing is therefore changed from use limitation based on compatibility of purposes to use limitation based on the justification criteria stemming from fundamental rights. Besides this change, the data protection framework includes also other types of use limitation such as limitation based on strict interpretations of the purpose specification that have been stipulated by the legislature. This stricter type of use limitation demonstrates that the data protection framework does not have a similar dependency on the non-incompatibility requirement than it has on the purpose specification requirement.

Chapter 6

Conclusion

This study took a doctrinal approach to the purpose limitation principle. It discussed the two components of the principle, the purpose specification requirement and the non-incompatibility requirement, separately. I took this approach because at the outset of the research for this study my hypothesis was that the purpose limitation principle was primarily of protective value in data protection law due to the non-incompatibility requirement. In my eyes the specification of purposes was a formality and an imperative step that had to be taken in order to prompt the protective value of the principle: the limitation of personal data processing based on the compatibility of purposes. I presupposed that this hypothesis was supported by the case law on data protection matters and the protection of fundamental rights of the CJEU and the ECtHR. Like other scholars, I even went as far as reading the non-incompatibility requirement implicitly in the wording of the purpose specification requirement as codified in art. 8(2) CFREU.

I was wrong.

By discussing the two requirements separately, I was able to untangle the purpose limitation principle and to look at its function in data protection and human rights law from a refreshing standpoint. This study has found that the protective value of the purpose limitation principle is primarily due to the significant role that the purpose specification requirement plays in data protection and fundamental rights law.

I have looked at two functions of the purpose specification requirement: the autonomous function, that prescribes that personal data is only processed for legitimate, explicit and specific purposes,[787] and the conditional function of the purpose specification requirement, that relates to the idea that the purpose specification requirement directly or indirectly affects the applicability, application and the outcome of other

[787] See Chapter 3 on page 57.

rules of data protection and fundamental rights law.[788] This latter function weaves the purpose limitation principle through the whole data protection framework. Under the conditional function, other data protection rules are dependent for their their applicability, application or outcome on the purpose specification requirement directly or indirectly by depending on the purpose specification or the processing purposes.[789]

Purpose limitation in fundamental rights law

The main findings of this study are presented in this conclusion as direct answers to the subquestions that were articulated in Section 1.3.3.

To what extent do limitations on the purpose specification requirement lead to infringements of fundamental rights? Limitations on the purpose specification requirement can lead indirectly and directly to infringements of fundamental rights. Limitations on the purpose specification requirement can lead indirectly to infringements of fundamental rights because the ECtHR takes into account all conditions of data processing when assessing if data processing falls under the ambit of art. 8(1) ECHR. In the assessment of whether or not data data falls under the scope of the concept *data relating to the private life of individual* the ECtHR takes into account the legal qualification of the data, the type of data and the type of data processing. The processing purposes will reveal, together with a description of the processing means, the necessary information to make this assessment. The purpose specification requirement therefore indirectly contributes to application of fundamental rights in day-to-day data processing operations.[790] When a data controller that is bound by the fundamental rights obligations that follow from the ECHR fails to respect the purpose specification requirement because the processing purposes are not legitimate, in the sense that purposes do not meet the standards that follow from the substantive conception of the legitimacy element, the data processing will directly lead to an infringement of art. 8(1) ECHR.[791]

[788] See Section 4.1 on page 89.
[789] See Section 1.3.1 on page 11 for the vocabulary that is used in this study.
[790] See Section 2.1.1.2 on page 25.
[791] See Section 3.3.2 on page 64.

In what way is the idea behind purpose specification connected to the justification criteria of fundamental rights infringements? The purpose specification requirement is connected to all justification criteria in fundamental rights law and plays a central role in the protection of fundamental rights in data protection law.[792] The *legitimate aim* of an interference is different from the processing purposes. The results of this study indicate, however, the processing purposes function as a starting point for the assessment of the legitimate aim of a restricting measure for both the ECtHR and the CJEU. The legality criterion *in accordance with the law* refers to the rule of law, meaning that an infringing measure should be based on accessible, foreseeable law that is encompassed with safeguards. The purpose specification requirement directly contributes to the foreseeability of restricting measures because it lays down that the processing purposes have to be explicit and specific and determined prior to the actual data processing. The purpose specification requirement is also connected to the execution of the proportionality assessment of a restricting measure because it can function as the specification of the processing circumstances in connection to the legitimate aim.

When it comes to data processing that would fall under the scope of the LED, this study has found that in data protection cases the ECtHR indirectly refers to purpose limitation when it demands that, firstly, infringements must be based on measures that codify the objectives for which the powers can be authorized, and, secondly, that the processing purposes of the concrete data processing operation must be specified prior to the authorization of the interfering measure.[793] For secret surveillance the necessary safeguards that should accompany an infringing measure consist of a clear indication of the nature of the offenses that might give rise to the measure, the category of people susceptible to the measure, the duration on the measure, the existence of effective supervision, limitations on the use of the collected data and effectuation of other data protection principles in domestic legislation.[794] When foreseeability is limited because the infringing measures ought to be kept secret in order to be effective, the conditional function of the purpose specification requirement increases because the safeguards that are put in place to balance the lessened foreseeability should be effective and adequate considering the overall processing purposes. The

[792] See Section 4.2 on page 117.
[793] See Section 4.2 on page 117 and Section 5.2.2.3 on page 159.
[794] See Section legality on page 162.

connection between the justification of infringements for objectives that are listed in art. 1(1) LED and the purpose specification requirement is, therefore, stronger than it is for data processing that falls under the scope of the GDPR.

To what extent is purpose specification connected to (the essence of) the fundamental right to respect for private life and the right to protection of personal data? The essence of the right to protection of personal data entails the minimum means that have to be put in place to enjoy effective protection of personal data. These means include at least the safeguarding of the integrity and confidentiality of personal data and the purpose specification requirement. The purpose specification requirement, therefore, belongs to the essence of the right to protection of personal data.[795]

Would the right to protection of personal data and the right to respect for private life be safeguarded if the purpose limitation principle would be replaced by other concepts to regulate the use of personal data? The purpose specification requirement is connected in such a way with the fundamental right to protection of personal data that the replacement of purpose limitation by other concepts, such as the interests of the data controller,[796] would affect the protection of various data protection principles and rules and it would lead to multiple problems in the assessment and mitigation of interferences with fundamental rights. Most glaringly, a replacement would lead to a violation of the essence of the right to protection of personal data.[797]

To what extent does further use of personal data lead to an infringement of fundamental rights? ***and*** **To what extent do limitations on the non-incompatibility requirement lead to an infringement of fundamental rights?** With regard to the non-incompatibility requirement and the fundamental rights framework, the following conclusions can be drawn: The further use of personal data does not in itself lead to an infringement on fundamental rights for data processing that would fall under the GDPR and data processing that would fall under the LED. The factors of the com-

[795] See Section 4.2.4 on page 124.
[796] This is suggested by Moerel and Prins. See Section 1.1.
[797] See Section 4.2.4 on page 124.

patibility requirement have been taken into account by the ECtHR when determining an infringement on art. 8(1) ECHR.[798] Further use of data solely within the context of criminal law enforcement has not amounted to a violation of the right to respect for private life; in the cases that would fall under the scope of the LED, the ECtHR has never discussed the re-use of personal data in light of art. 8(1) ECHR.[799] A similar conclusion can be made from the case law of the CJEU, that systematically omits reference to the non-incompatibility requirement in its reasoning on the establishment and impact of infringements of art. 7 and 8 CFREU, and instead, refers to various other data protection principles.[800]

In what way is the non-incompatibility requirement connected to the justification criteria for fundamental rights infringements? Limitations on the non-incompatibility requirement and limitations on the accompanying compatibility assessment under data protection law do not lead to infringements or violations on fundamental rights when considering the legitimacy of further processing of personal data.[801] The circumstances that surround the further processing can contribute to the establishment and the impact of an infringement on fundamental rights. This study showed that for cases that would fall under the scope of the GDPR the ECtHR has used similar factors to those of the compatibility assessment when considering the circumstances of data processing and for the establishment and impact of infringements of art. 8(1) ECHR in cases that concerned the further processing of data relating to private life. These factors were, however, never applied in a cohesive manner that resembled a compatibility test. The case law of the ECtHR can, nevertheless, be of help in the further substantiating of the compatibility assessment under the GDPR. When it comes to the justification criteria of interferences with fundamental rights both courts have referred to the non-incompatibility requirement in the assessment of safeguards that mitigated the negative effects of data processing that the courts connected to restrictions on the fundamental rights or other data protection principles.

[798] See Section 5.1.3 on page 145.
[799] See Section 5.2.2.3 on page 159.
[800] See Section 5.1.2.2 on page 139.
[801] See Section 5.2.2.3 on page 159.

Purpose limitation in data protection law

The answers to the subquestions on the role of the purpose limitation principle in European data protection law are as follows:

What is the role of the purpose specification requirement in data protection law? The purpose specification requirement plays a central role in data protection law. It is one of the core data protection principles.[802] The principle has made it possible for the legislature to build a data protection system that uses the purpose specification and the actual processing purposes as input for other decisions regarding the protection of personal data. Under the GDPR the purpose specification requirement has an autonomous function as a safeguard in the protection of rights and freedoms of the data subject in vertical and horizontal relationships. Under the LED this autonomous function is primarily extended as a safeguard in the protection of rights and freedoms of the data subject in vertical relationships and should solely be attributed to the purpose specification requirement because use limitation is dominated by the derogation clause of the non-incompatibility requirement based on similar criteria that should also be applied under fundamental rights obligations of States.[803]

The processing purposes point towards the data controller and the data processor, and towards the supervisory authority, specifically in cross-border processing operations. With that, the purposes are one the factors that should be taken into account when determining who is accountable for the data processing and in which jurisdiction a supervisory authority enforces the European data protection framework.[804]

This research results in the conclusion that the other data protection principles are directly dependent on the purpose specification requirement for its position as one of the data protection principles that provides the protection in data processing operations. The other data protection principles also have a high dependency on the processing purposes for their application and outcome.[805] Indirect dependency can be seen for the character and proportionality of the enforcement of the data protection framework by the supervisory authority on both the purpose specification and

[802] See Section 4.3 and 5.2.1.1. See also Section 4.2.4 on page 124.
[803] See Section 5.5.2 on page 183.
[804] See Section 4.1.1.1 and Section 4.1.1.3.
[805] See Section 4.1.3 on page 102.

the actual processing purposes.[806] The role of receiver and recipient is determined by the purpose specification and the actual processing purposes too.[807] The role of recipient or receiver affects the transparency obligations of the disclosing data controller with regard to keeping track of the disclosures and providing information about them, as well as the applicability and application of certain data subject rights. Whether a public authority to whom personal data is disclosed qualifies as a recipient or as a receiver can be determined by looking at the purpose specification that is embedded in the legal statute that underlays the competence of the public authority to receive the personal data and by looking at the actual processing purposes to determine whether or not the personal data will be used for a particular inquiry by that public authority. For voluntary disclosures, one of the rationales of this study, no legal obligation is underlying the transfer, and the competent authority to whom the data is disclosed by a private entity can therefore not qualify as a receiver and should instead be considered a recipient of the personal data. In general the data subject has more rights and the data controller has more transparency obligations when personal data is disclosed to a recipient.

The multiplicity of necessity and proportionality assessments in data protection law depend on the processing purposes and are therefore indirectly dependent on the purpose specification requirement.[808] The answer to the necessity question that is embedded in the application of the lawful processing ground is dependent on the processing purposes: *Is personal data the type of information that should be processed in order to pursue the processing purposes?* The answer to the subsidiarity question, that comes after the question on necessity to process any personal data at all, depends on the processing purposes too: *Is it necessary to process this personal data to pursue the processing purposes?* And the proportionality question on the duration and extent of the processing operation is dependent on the processing purposes: *Is the processing operation limited to the minimum necessary to fulfill the purposes of processing?* The application of the lawful processing grounds to a data processing operation is dependent on the processing purposes too, including the lawfulness of processing for privileged purposes and processing of special categories of personal data.[809] This study has also argued that the processing purposes condition the rights of the data subject

[806] See Section 4.1.6 on page 116.
[807] See Section 4.1.1.2 on page 92.
[808] See Section 4.1.2.1 for these questions.
[809] See Section 4.1.2 and Section 4.1.5.5.

in automated decision making, objection procedures and erasure requests, and that therefore the applicability and application of these rights are indirectly dependent on the purpose limitation requirement.[810] The conditional function of the purpose specification requirement is expanded with the coming into force of the new regulatory framework. The novelties of the GDPR and the LED all depend on the processing purposes for their effectuation and application: the appointment of a data protection officer, the data protection impact assessment, the specified security obligations and the implementation of data protection by design and by default.[811]

What is the role of the non-incompatibility requirement in data protection law? The non-incompatibility requirement regulates use limitation based on the compatibility of purposes. The requirement demands a compatibility assessment between the initial purposes – the processing purposes at the moment of data collection or re-use of personal data – and the new purposes, which are any secondary processing purposes that are different from the initial purposes.[812] If this test is passed, the personal data can be further processed for the compatible yet new purposes. The GDPR compatibility test includes an assessment of the link between the purposes, context of processing, nature of the data, possible consequences of the processing on the rights and freedoms of the data subject and safeguards to mitigate the potential negative consequences.[813]

The separated discussion of the two requirements revealed that the relationship of the non-incompatibility requirement with other rules and principles in data protection law is different from the relationship between the purpose specification requirement and these other rules and principles. The non-incompatibility requirement fulfills no conditional function. In other words, other principles and rules can properly function when derogations are made from the non-incompatibility requirement, or when other types of use limitation apply such as use limitation based on a strict interpretation of the processing purposes that are stipulated by the legislature or data controller.

What is the relationship between the purpose specification requirement and the non-incompatibility requirement? When looking at the relationship of the non-

[810] See Section 4.1.4 on page 108.
[811] See Section 4.1.5 on page 112.
[812] See Section 1.3.1 of the introductory chapter for the definitions and vocabulary of this study.
[813] See Section 5.1.1 on page 131.

incompatibility requirement and the purpose specification requirement, we see a dependency of the former on the latter, which is not *vice versa*. The purpose specification requirement can function perfectly in conjunction with other forms of use limitation than use limitation based on the compatibility of purposes, while the non-incompatibility requirement is dependent for its applicability on the purpose specification requirement.

What is the position of the purpose limitation principle as a data protection principle compared to the position of the other data protection principles? One unanticipated finding of this study was that the two requirements of the purpose limitation principle end up on very different positions in relation to the other data protection principles. The purpose specification requirement belongs the essence of the right to protection of personal data and can under no circumstances be restricted, and the non-incompatibility requirement knows a system of derogations that do not have to be interpreted as an exception to the rule of non-incompatibility, but instead contribute to the system of use limitation in data protection law.

The results of this study support the idea of a hierarchy in data protection principles. All data protection principles must be respected in order for data processing to be lawful under the European data protection framework. However, for some principles restrictions or derogations are permitted, while for others these are not.[814] The purpose specification requirement of the purpose limitation principle, the fairness, lawfulness, and integrity and confidentiality principle cannot be restricted.

This study has argues that the purpose specification requirement and the integrity and confidentiality principle have been brought in connection with the means necessary to protect the essence of the right to protection of personal data by the CJEU.[815] For this reason this requirement and this principle cannot be restricted under any circumstances. It is yet to be determined in the case law of the CJEU whether the fairness and lawfulness principles enjoy a similar status. The transparency-, data minimization-, accuracy and storage limitation principles can be restricted under the general restriction clause of art. 23 GDPR.[816] The results of this study suggest that the non-incompatibility requirement of the purpose limitation principle cannot be re-

[814] See Section 5.2.1.2 on page 154.
[815] See Section 4.2.4 on page 124.
[816] See Section 5.2.1.2 on page 154.

stricted, but the data protection framework does permit derogations from the rule of cumulation of the lawful processing grounds and this requirement.[817] From the case law analysis can be concluded that restrictions on data protection principles should always be an exception, that cannot form the general rules for data processing.[818] For derogations from the non-incompatibility requirement no similar conclusion can be drawn because in its judgements the CJEU does not pay attention as to whether data processing is based on such a derogation or not.[819]

What other types of limitations on data processing are implemented in European data protection law? This study has identified that – besides use limitation based on the compatibility of purposes – the data protection framework foresees in use limitation based on the justification criteria stemming from fundamental rights,[820] use limitation based on privileged purposes,[821] and use limitation based on stringent interpretations of the purposes that are stipulated by the legislature of data controller.[822] Under the GDPR the derogations on the non-incompatibility requirement should be based on renewed consent or a *lex specialis* as required in art. 6(4) GDPR.[823] The derogation on the non-incompatibility requirement pursuant to a *lex specialis* that is based on art. 6(4) GDPR and its execution should meet the justification criteria stemming from fundamental rights law.[824] For data processing under the GDPR, this results in default use limitation based on compatibility of purposes, because not all data controllers will receive consent from the data subject for the re-use, and not all re-use will pass the justification criteria stemming from fundamental rights law as embedded in art. 6(4) GDPR.

For data processing under the LED, a different conclusion should be drawn. Derogations from the rule of cumulation under the LED are only permitted for re-use that meets the justification criteria stemming from fundamental rights law ex art. 4(2) LED. This study has found that almost all processing of personal data by competent authorities, regardless of it being for initial or new processing purposes, has to meet

[817] See Section 5.2.2 on page 156.
[818] See Section 5.2.2.1 on page 156.
[819] See Section 5.1.2.2 on page 139.
[820] See Section 5.5 on page 181.
[821] See Section 5.6 on page 189.
[822] See Section 5.7 on page 193.
[823] See Section 5.3 and Section 5.2.2.1.
[824] See Section 5.2.2.3 on page 159.

the justification criteria stemming from human rights law because it interferes with the rights and freedoms of the data subject.[825] One of the more significant findings to emerge from this case law analysis is that the criteria for processing for initial purposes and processing for new purposes are the same. This changes the default use limitation on personal data processing under the LED from use limitation based on compatibility of purposes to use limitation based on the justification criteria stemming from fundamental rights law.[826]

How does the non-incompatibility requirement relates to these other types of use limitation? The derogations to the non-incompatibility requirement should be interpreted as part of the system of use limitation in data protection law. Use limitation based on other types of use limitation do not make an exception, but form an integral part of the protective scope of the European data protection framework.[827] It is important to note however, that once data is re-used for a new incompatible purpose, use limitation based on the compatibility of purposes regains its role. This role is bigger under the GDPR than it is under the LED.

What is the relationship between the purpose specification requirement and these other types of use limitation? This study has found that all types of use limitation depend directly or indirectly on the purpose specification requirement. By replacing the purpose limitation principle for a different type of default use limitation while not taking the role of the purpose specification requirement into proper regard, not only use limitation based on compatibility of purposes would be affected, all other types of use limitation would be too because of this dependent relationship on the purpose specification requirement. This dependency is, however, one-directional. The purpose specification principle does not depend on specific forms of use limitation to function.

[825] See Section 5.5.2 on page 183.
[826] See Section 5.5.4 on page 187.
[827] See Section 5.2.2.3 on page 159 and Section 5.1.2.2 on page 139.

Purpose limitation in voluntary data transfers between private entities and criminal law enforcement authorities

In Section 1.1, the introduction chapter of this study, several question were raised regarding role of the purpose limitation principle in various data transfers from private parties to criminal law enforcement authorities for the detection, prevention and investigation of crime: What is the role of the purpose limitation principle when a legal obligation to transfer the data to the criminal law enforcement authorities is missing but data is nevertheless voluntarily transferred? What is the role of the purpose limitation principle when a private entity spontaneously discloses personal data of individuals to the police because the entity suspects that the data will reveal fraudulent conspiracy? What is the role of the purpose limitation principle when the private entity is confronted with a request instead of a warrant, and it transfers bulk data to the criminal law enforcement authority? And what is the role of the principle when a criminal law enforcement authority buys access into the database of a private entity? The findings of this study contribute to the answer of these questions and to the general understanding of the purpose limitation principle in the voluntary disclosure of GDPR-data by private entities to competent authorities for purposes that pursue criminal law enforcement objectives. Again, the main findings of this study will be presented as answers to the subquestions that were formulated in Section 1.3.3.

How are voluntary data transfers of GDPR-data for LED objectives regulated in the European data protection framework? Voluntary data transfers of GDPR-data by private entities to competent authorities for LED objectives are regulated through Recital 50 GDPR.[828] The data protection framework does not include a derogation from the rule of cumulation between the non-incompatibility requirement and the processing ground that is mentioned in Recital 50 GDPR: art. 6(1)(f) GDPR.[829] This means that the voluntary cooperation with competent authorities must be specified prior to the data collection and communicated with the data subject, otherwise the data transfer will violate the non-incompatibility requirement and the data controller

[828] See Section 5.4.2 on page 175.
[829] See Section 5.2 and 5.3.

is not fulfilling her transparency obligations.[830] There are several limitations dictated with regard to the characteristic of the type of data transfer that can be based on art. 50 GDPR: the recital allows the *ad hoc* transfer of personal data that relates directly to one or more individuals, but not the transfer of bulk data for the purposes of detection, prevention and investigation of crime that does not relate to a specific or a series of criminal events. Overall, Recital 50 GDPR is meager compared to the fundamental rights challenges posed by data-driven society'. The European legislature could have been more specific on the types of data transfers that are included in this recital in order to give the new regulatory framework more longevity. Specifically the issue of data-driven policing and profiling for the objective of criminal law enforcement could have been more detailed by the legislature. Currently it is unclear whether the transfer of data that is selected because it meets a general profile could fall under the scope of Recital 50.[831] If it would, questions on the adequacy of safeguards and checks and balances immediately arise.[832]

This study illustrated that the competent authority that recieves the data from a voluntarily cooperating private entity should be considered a recipient. The transferring private entity should therefore be transparent about and keep track of the transfers. The data subject rights are not restricted under the GDPR for data transfers to recipients, which means that the data controller cannot secretly and voluntarily transfer data to competent authorities in the pre-crime phase of criminal law enforcement.[833]

To what extent can private entities determine the processing purposes and restrict the processing by the criminal law enforcement authority after data is voluntarily transferred? Regardless of the legality of the data transfer, once data has been transferred by private entities to criminal law enforcement authorities to be processed for a purpose that pursues one of the objectives as listed in art. 1(1) LED, the private entity looses all control over the purposes for which the data is transferred. Limitations on the use of transferred data are no longer based on the compatibility of purposes at the moment of transfer but on the justification criteria stemming from fundamental rights because the criminal law enforcement agency can base the re-use

[830] See Section 5.4.2 on page 175.
[831] See Section 5.4.3 on page 5.4.3.
[832] See Chapter 8 for suggestions on further research that would address this issue.
[833] See Section 4.1.1.2 on page 92.

after the transfer on art. 4(2) LED.[834] The private entities have, therefore, no control over the processing purposes once the data is transferred.

Do the purposes of processing of the private entity affect the lawfulness of the data collection by the criminal law enforcement authority when this data is voluntarily transferred by the private entity? The European legislature was clear about the purpose limitation principle in data transfers that are based on an obligation for the private entity: the processing operation of receiving the data by the competent authority is the initial processing and, therefore, the competent authority can determine the processing purposes.[835] With regard to voluntary data processing such statements have not been made.[836] The absence of specific reference to voluntary data transfers in this context could be due to the lack of attention given to public private partnerships during the legislative process of the new regulatory framework. The finding could also suggest that the incompatibility of purposes of the voluntary data transfer with the initial purposes influences the lawfulness of the data collection by the competent authority. If this is the case, the fundamental rights framework provides the answer to what extent the unlawfulness of the data processing by the private entity falls under the accountability of the government.

Under which conditions stemming from fundamental rights law does processing by a private entity of data that is intended for transfer to a competent authority fall under the accountability of the government? In determining the accountability of a State for infringements by private entities in public-private partnerships, the ECtHR looks at the engagement of both parties and takes into account the durability of the cooperation, the contributions of the authorities, the association of the criminal law enforcement authorities with the infringing actions and the extent of control over the actions of the private entity. This could mean that even though the private entity should be considered the data controller under data protection law, the involved competent authority to whom the data is disclosed can be held accountable for actions of the private entity that infringe art. 8(1) of the ECHR.[837] These criteria might be fulfilled in situations where the criminal law enforcement authority buys access into

[834] See Section 5.5 on page 181.
[835] See Section 2.2.2.3 on page 54.
[836] See Section 5.4.3 op page 179.
[837] See Section 2.1.1.4.2 on page 31.

the database of the private entity and the private entity and criminal law enforcement authority communicate about the type and sources of personal data that is added to the database by the private entity, duration of retention or type of storage of the data.

Answer to the main research question

As to the main research question of this study:

> *What is the role of the purpose limitation principle in European data protection and fundamental rights law?*

The role of the purpose limitation principle cannot be explained without separating the two different requirements because both requirements have a distinctively different role in fundamental rights and data protection law. The purpose specification requirement is one of the foundations on which the data protection framework has been built and the principle contributes to application of fundamental rights in day-to-day data processing operations. The purpose specification principle cannot be restricted and there are no derogations from the application of this principle. If there were the whole protective system of data protection would collapse like a house of cards. The non-incompatibility requirement, on the other hand, is a simple data protection rule with limited scope and function. The non-incompatibility requirement knows various derogations and is just one of the types to limit the use of personal data under European data protection law. This is not to say that within its limited scope and function the non-incompatibility requirement does not play an important role in the European system of data protection. I would highly recommend to address the two requirements of the principle separately in future discussions about the purpose and limitations of purpose limitation.

Chapter 7

Recommendations

To the European legislature:

In the year 1998 the Signatory States to the DPC deemed it "neither desirable nor possible to strive for a far-going harmonization of data protection rules for criminal data."[838] With the development of the data-driven society, these rules became desirable and twenty years after this statement was published the DPDP came into effect. Now, the European legislature is convinced that no separate rules are necessary to regulate data transfers from private entities to competent authorities.[839] Given the conclusions of this study and the fundamental rights aspirations of the Union I would suggest reconsidering this position prior to future revisions of the European data protection framework. With the further development of the data-driven society the data transfers from private entities to criminal law enforcement authorities for the detection and prediction of crime will increase. A key policy priority should therefore be to clarify the framework on voluntary data transfers from private entities to criminal law enforcement authorities for the detection and prediction of crime.

To civil society:

I have argued that the legal framework prohibits voluntary transfers of bulk data from private entities to criminal law enforcement authorities. I have also questioned the legality of voluntary data transfers based on matches with general profiles. This information can be used to develop strategic litigation procedures based on art. 79

[838] Second Report R(87)15, 1998, p. 5.

[839] See Section 5.4.1 that discusses the standpoints of the various branches of the EU legislature on this topic.

and 80 of the GDPR in order to challenge the data broker industry that caters to criminal law enforcement for the detection and prediction of crime.

Chapter 8

Future research

The introduction on page 9 explained that not all public-private partnerships in data-driven criminal law enforcement concern the transfer of personal data, some will concern the transfers of general profiles. Despite the fact that prior to general profile transfers personal data is processed for the composition of the general profile, and that after the transfer the information of the general profile qualifies as personal data when it is used to single out natural persons and to add information to personal profiles, the purpose limitation principle does not regulate these transfers because the general profile itself does not consist of personal data and during the transfer no personal data is processed. More research is needed to understand the fundamental rights implications of the transfers of general profiles. Future work could also be carried out to establish the effect of territorial jurisdiction in data protection on the legality of criminal law enforcement. A greater focus on predictive policing, profiling and big data could produce interesting findings that account more for the effects on group privacy as well as transparency. Considerably more research is needed on predictive policing systems from the criminal law enforcement legality point of view.

An issue that was not addressed in this study was whether a business model that is based on catering data to law enforcement authorities can pass the legitimate interest test of art. 6(1)(f) and if the processing purposes at the time of collecting the data qualify as legitimate. I felt that the answers to these questions rely too heavily on the circumstances of the case and required additional research. Future research on this topic is desirable.[840] Research is needed on the scope of Recital 50 GDPR in relation to data transfers based on profiles. More specifically research is suggested that would look into the necessary safeguards and checks and balances that follow

[840] For those who want to take up this task, I have prepared a series of use cases that can function as a starting point for this research. Please contact me.

from fundamental rights law transfers data that is selected because it meets a general profile. Future research might discuss the horizontal effect of fundamental rights in data transfers from private entities to criminal law enforcement agencies for the detection of crime, as well as the retrospective application of the right to a fair trail on the data processing by the private entity.

Future research into the purpose limitation principle in data transfers between different competent authorities, intelligence agencies and European law enforcement agencies such as Europol is recommended. Future work could usefully explore the purpose limitation principle in predictive policing by Europol.[841] Public-private partnerships and data transfers between non-criminal law enforcement agencies, such as administrative agencies charged with social security fraud detection, fell outside the scope of this study. It would be interesting, however, to take the conclusions from this study and investigate to what extent these hold for such personal data transfers. Future research might also explore the use of transferred data for purposes that fall outside the scope of EU law.

An important part of the protection of the right to personal data is in the hands of national data protection authorities. Future research into the interpretations of the purpose limitation principle by the national data protection authorities is recommended and could contribute to the consistent interpretation of data protection law throughout the European Union.

[841] See for an investigation of the implementation of the purpose limitation principle in the Europol Regulation. [Coudert, 2017].

Acknowledgements

In 2011 I was asked whether I was interested in a PhD position with a new interdisciplinary research lab, called the Privacy & Identity Lab (PI. Lab). I was over the moon. I imagined having interesting discussions on law and technology while deepening my knowledge on the law and broadening my technological skills. It was all that and much more.

I would like to express my deep gratitude to my supervisors Mireille Hildebrandt and Bart Jacobs. Mireille, thank you for your continuous support, inspiration, encouragement, supervision, knowledge and kindness. Bart, thank you for offering this position and your sharp feedback.[842]

I would like to express my gratitude to the members of the Doctoral Thesis Committee: Frederik Zuiderveen Borgesius, Janneke Gerards, Natali Helberger, Marion Oswald and Gabriela Zanfir-Fortuna, as well as all members of the Doctoral Examination Board.

I am grateful to Eben Moglen, who invited me to Columbia Law School in New York, where I stayed for six months in 2015 and conducted research for this study. I would like to thank Janneke Gerards for her guidance on the particularities of the

[842] In 2013 Minister of Security and Justice Opstelten won the Big Brother Award, an award for the institution that has done most to threaten privacy. The award was not collected by the minister during the award show. Later that year I dared Bart to present to Minister Opstelten this uncollected award at a dinner party. In return I would put Bart twice in the acknowledgements of this study. Here you go: Thank you Bart!

human rights law legal discipline. I thank my colleagues at the PI. Lab and at the Radboud University, in particular Jaap-Henk Hoepman, Paulan Korenhof and Greg Alpár.

I could not have done this research without the financial aid of the SIDN fonds. Thank you. I am thankful to Emmanuel Goldstein and Stichting Internet4All for their support during my stay at Columbia Law School.

My special thanks are extended to my friends and family. I am very much indebted to Marion and Michiel. Marion, I want to thank you for your unconditional love and support. You are an inspiration and a guide in my life. Michiel, thank for your support and affection.

Finally, I wish to thank Fabienne. Never have I felt the positive effects of the data-driven society more, than when an algorithm matched our online profiles. Thank you for your support during the last phases of this study. The future is bright with you.

Summary

This study focuses on the purpose limitation principle, which prescribes that personal data should only be collected for specified, explicit and legitimate purposes and should not be further processed in a manner incompatible with those purposes. This principle has two components: the purpose specification requirement and the non-compatibility requirement. The non-incompatibility requirement is a type of use limitation. For the purpose of this study, the two requirements will be examined independently of each other.

Data protection law knows multiple types of use limitation, all of which are discussed in this study, including use limitation derived from the non-compatibility requirement. This study is limited to European law, which includes the law of the Council of Europe (CoE) and the European Union (EU). The results of this study are based on desk research into the relevant sources of law: legislation, case law, doctrine, and opinions and guidelines of the European Data Protection Board and other advisory bodies.

Background and central research question

The rationale for this study is twofold.[843] On the one hand, there is increasing criticism of the purpose limitation principle. The principle is considered outdated and

[843] Summary based on Section 1.1 of this study.

difficult to reconcile with the data-driven society of big data analysis and artificial intelligence. I have to agree to this because in the design decisions of the latter two technologies the purpose limitation principle is taken little into account at present. This can prove difficult for the person responsible for the deployment of such technologies on the European market because the purpose limitation principle is legally binding. On the other hand, the use of algorithmic decision models in combination with data analysis, such as profiling, is emerging within the field of criminal law enforcement. So called *predictive policing* systems are developed for and by law enforcement authorities. These systems analyze (bulk) data sets for the detection of criminal offenses in the early stages of criminal proceedings. There is a risk that the input for these systems will consist of (bulk) data collected by commercial parties for a purpose other than the detection of criminal offenses. This creates tension with the purpose limitation principle.

Some scientists have suggested replacing the purpose limitation principle with a system based on the interests of the data controller; instead of the processing purposes, the interests of the data controller will then be at the centre of the considerations on further processing of personal data. Before looking for an alternative to the purpose limitation principle, it is important to understand if an alternative should be sought at all and, if so, for what purpose. This study therefore focuses on the purpose and limitations of the purpose limitation principle.

The central research question is therefore:

> *What is the role of the purpose limitation principle in European data protection and fundamental rights law?*

Relevant legal framework

The following legislation and treaties are important for this study:

At the level of protection of fundamental rights, Article 8 of the European Convention on Human Rights (ECHR) and Articles 7 and 8 of the Charter of Fundamental Rights of the European Union (CFREU) are mainly relevant to this study.

The European Court of Human Rights (ECtHR) uses the concept of *data relating to private life* to rule in cases that concern processing of data and that constitute an

interference with the first paragraph of art. 8 ECHR.[844] Three factors play a role in the qualification of data relating to private life. First, there is the legal qualification of the data, such as the qualification of sensitive personal data, for example health data or data about someone's ethnicity, and the qualification of data about criminal convictions or offenses. Secondly, the type of data plays a role. Examples are location data, DNA data, portraits, communication data and financial data that have been brought within the scope of art. 8(1) ECHR several times by the ECtHR. The third factor is the type of data processing. An example of this factor is the monitoring of behavior or the creation of personal profiles. The case law of the ECtHR shows that the application of data protection safeguards is without prejudice to the outcome of the question whether data processing falls under the ambit of art. 8(1) ECHR.[845]

Only a few times the ECtHR dealt with cases in which an interference with art. 8(1) ECHR had been committed by a private entity that did not work on commission but in cooperation with investigative authorities.[846] In those cases, the ECtHR considered the following aspects: durability of the cooperation, the contributions of the authorities, the association of the criminal law enforcement authorities with the infringing actions and the amount of control of the authorities over the actions of the private entity. Interference with the first paragraph of art. 8 ECHR must meet the cumulative criteria of the second paragraph of that same article in order to be justified under the Convention. The interference must pursue a legitimate aim, must be in accordance with the law, and must be necessary in a democratic society.

The CFREU applies to legislative and implementing acts of the EU institutions, bodies, offices and agencies and to acts of the Member States when they are implementing EU law.[847] The entry into force of the Lisbon Treaty in 2009 has changed three things in European data protection law. First, a fundamental right to the protection of personal data is established, as laid down in art. 8 CFREU, which functions independently of the right to privacy, as protected under art. 7 CFREU. Secondly, the role of the CJEU has changed as it has been explicitly given the task of monitoring the observance of fundamental rights in the EU. Thirdly, the scope of European data protection law has been widened. It now includes the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or

[844] Summary based on Section 2.1.1.2 of this study.
[845] Summary based on Section 2.1.1.3 of this study.
[846] Summary based on Section 2.1.1.4 of this study.
[847] Summary based on Section 2.1.2 of this study.

prosecution of criminal offenses or the execution of criminal penalties, including the protection against and prevention of threats to public security.

Article 7 CFREU lays down the right to protection for private life and is almost identical to art. 8 ECHR. The first paragraph of art. 8 CFREU guarantees the fundamental right to the protection of personal data. This right is further specified in the second and third paragraphs of art. 8 CFREU. Article 8(2) CFREU defines two rights for the data subject: the right of access and the right to rectification of the data. It also lays down three conditional criteria for the processing of personal data: data must be processed fairly, for specified purposes and with the consent of the data subject or on any other legitimate basis provided for by law. These conditional criteria are linked to the following data protection principles: the purpose specification requirement, the principle of fairness and the principle of lawfulness. The third paragraph lays down the guarantee of independent oversight. The case law shows that the CJEU applies the rights set out in articles 7 and 8 CFREU in conjunction as *the right to respect for private life with regard to the processing of personal data*.

The relevant data protection law consists of the revised version of the Data Protection Convention of 2016 (DPC), Recommendation (87) 15 regulating the use of personal data in the police sector (R (87) 15), the General Data Protection Regulation (GDPR) and the Data Protection Directive on Police Matters (LED).

General idea of the purpose limitation principle

Purpose limitation reduces data processing to procedures with a clear beginning and end point.[848] The processing must be designed to achieve the processing objectives. As soon as the purpose has been exhausted, the lawfulness of the processing expires. Different scientists assign different roles to the purpose limitation principle. These roles include transparency, legal certainty, distribution of power, integrity, dignity, equality, autonomy, informational self-determination, support for democracy, and a fair trial.[849] These roles assume that the principle functions as a safeguard in vertical and horizontal relations between those responsible and those subjected to the data processing. The purpose limitation principle has six elements of relevance.[850]

[848] Summary based on Section 3.1 of this study.
[849] Summary based on Section 3.4 of this study.
[850] Summary based on Section 3.3 of this study.

First, the element of a *processing purpose*, in short a *purpose* is relevant. The purpose is usually the answer to the question: "Why is personal data processed?". This question often coincides with the question: "How is the personal data processed?" which oversees the means of processing. The processing purposes should be sufficiently clear to support decisions on the proportionality of the data processing. Preferably, the purposes should be laid down in a written purpose specification, so that they can be communicated to all parties concerned, including the supervisory authority when necessary.

Secondly, the element of *legitimacy* plays a role. A legitimate purpose is an independent concept which goes beyond a plain verification of the lawfulness of the processing. The purposes of processing must meet the requirement of *in accordance with the law*, and the processing must comply with *state of the art* technology and social and cultural norms. The responsibility for the justification of the purposes lies with the controller.

The third element is the *specificity* of the purpose. This implies that the legitimate purposes must be precisely and fully articulated so that any data subject, including those without legal or technical knowledge, can assess which processing is and which processing is not included in the procedure. Within the English-speaking scientific field, uncertainty has arisen as to whether the specificity element points to specific purposes or to specified purposes. The former relates to well-formulated purposes that point to the outcome of processing, and the latter only points to purposes that point to the process of processing. Specified purposes lack the capacity of norm-setting, and can therefore not fulfill the communication function of the *specificity criterion*, nor can the purposes serve as a factor in other proportionality decisions within data protection law. As a result, the specificity criterion is closer linked to specific purposes than it is to mere specified purposes. There is one exception in data protection law to the rule of specific purposes for the processing of personal data for scientific purposes. Under the GDPR, it is possible to give data subjects the opportunity to consent to the processing of their personal data within certain fields of scientific research, without the specific purpose having been defined in advance.

In the fourth place, the purposes should be explicitly defined. This element can only be found in EU law. The purposes should be clearly stated so that all parties can form a common understanding of the expected data processing. Preferably, the

purposes should be laid down in a written purpose specification.

Timing is important for the purpose limitation principle. This is the fifth element. The purposes should be specified prior to the start of the data processing.

The last element concerns the compatibility of the initial purpose of data collection with the purposes of further processing. This element is directly linked to the requirement of non-incompatibility and is substantiated in a test with the following factors:

- The relationship between the purposes for which the personal data has been collected and the purposes of the intended further processing.
- The context in which the personal data has been collected, in particular as regards the relationship between the data subjects and the controller and including the reasonable expectations of the data subjects based on their relationship with the controller as regards the further use of the data.
- The nature of the personal data, in particular whether special categories of personal data is processed or whether personal data relating to criminal convictions are processed.
- The possible consequences of the envisaged further processing for data subjects.
- The existence of appropriate safeguards in both the original and the intended further processing, which may include encryption or pseudonymisation.

Data processing must meet four conditions in order to be lawful.[851] First, the processing must comply with the data protection principles, including the purpose limitation principle. Secondly, the processing must be based on a lawful processing ground. Thirdly, the controller must comply with the data controller obligations. Finally, the data subject must be enabled to exercise her rights. These conditions are cumulative, which means that in general, the purpose limitation principle cannot be overridden if the controller bases the further processing on a new lawful processing ground. There are two exceptions to this rule of cumulation which are discussed later in this summary.

[851] Summary based on Section 3.5 of this study.

Purpose specification requirement

The purpose specification requirement has two functions: an autonomous function reflecting the concept set out in the previous paragraphs, and a conditional function, where the requirement directly or indirectly affects the applicability, application and outcome of other rules within data protection law.[852] Direct dependency means dependence on the requirement and its status within data protection law as a component of a prominent data protection principle: the purpose limitation principle. The data protection principles are directly dependent on the purpose specification requirement and its status as principle.[853]

Indirect dependence refers to the dependency of other rules of data protection law on the purposes of processing or on the purpose specification. This indirect dependency exists for the allocation of roles under data protection law, including the roles of controller, processor, recipient and the competent leading supervisory authority.[854] The conditional function of the purpose specification requirement also extends to the application of the lawful processing grounds since these depend on the purposes of processing and, where appropriate, on the purpose specification itself.[855] The processing purposes also determine the application and outcome of the right to erasure of data, the right to object and the right not to be subject to a decision based solely on automated processing which produces legal effects or significantly affects the data subject in any other way.[856] With the entry into force of the new regulatory framework in the EU in 2016, the conditional function has been extended. The responsibilities to be fulfilled by the controller increasingly depend on the purposes of the processing.[857] These responsibilities include the data protection by design and by default, the carrying out of a data protection impact assessment, the security of the processing, and the appointment of a representative in the EU and of a Data Protection Officer. The purposes also determine whether the processing qualifies for the special regime for data processing for privileged purposes of public interest archiving, scientific or historical research or statistical purposes.[858] The nature of the enforcement and the balance of

[852] Summary based on Section 4.1 of this study.
[853] Summary based on Section 4.1.3 of this study.
[854] Summary based on Section 4.1.1 of this study.
[855] Summary based on Section 4.1.2 of this study.
[856] Summary based on Section 4.1.4 of this study.
[857] Summary based on Section 4.1.5 of this study.
[858] Summary based on Section 4.1.5.5 of this study.

proportionality in the enforcement by the supervisory authority shall depend on the purposes of the processing and the purpose specification whether or not it has been drawn up by the controller.[859]

At first glance, the ECtHR does not seem to refer to the purpose limitation principle in its rulings. However, when taking a closer look the principle is ubiquitously but subtly reflected in the consideration regarding the existence and weight of an interference with the first paragraph of Article 8 ECHR.[860] In addition, both the CJEU and the ECtHR pay attention to the purpose specification requirement when assessing the three justification criteria for the protection of fundamental rights. The legitimate aim pursued by an interference is a different concept from the processing purpose. The latter is in many cases the starting point of the determination of the legitimate aim in the processing of data relating to private life.[861] The criterion in accordance with the law encompasses the quality of the law, including the accessibility and foreseeability of an interference. The purpose specification plays an important role in this.[862] The purpose specification requirement is conditional for the proportionality assessment associated with the application of the criterion: necessary in a democratic society.[863] An unexpected outcome of the study on the purpose limitation principle is that the purpose limitation requirement is at the core of the fundamental right to the protection of personal data due to its autonomous and conditional function within data protection law and the role it plays in the protection of fundamental rights.[864] This requirement can under no circumstances be limited. The limitation of the purpose specification requirement is an intolerable interference with the right to the protection of personal data.[865]

Use limitation

Multiple forms of use limitations exist in the European data protection framework.

[859] Summary based on Section 4.1.6 of this study.
[860] Summary based on Section 4.2 of this study.
[861] Summary based on Section 4.2.1 of this study.
[862] Summary based on Section 4.2.2 of this study.
[863] Summary based on Section 4.2.3 of this study.
[864] Summary based on Section 4.2.4 of this study.
[865] Summary based on Section 4.3 of this study.

Use limitation based on compatibility of purposes

The most common type of use limitation is limitation based on the compatibility of the purposes of further processing with the purpose at the time of collection of the data. This type of restriction is directly linked to the requirement of non-incompatibility of the purpose limitation principle. It enforces a compatibility test.[866] In this test, the new and initial purpose must be tested against the factors listed on page 224 for data processing that falls under the GDPR.

These factors can be found in the reasonings of the ECtHR in cases concerning further processing of data relating to private life.[867] This case law can, therefore, be used to further flesh out the factors of the compatibility test. The LED includes no further explanation of the application of this non-incompatibility requirement.[868] Further explanation is also lacking in the DPC that applies to data processing that falls within the scope of the GDPR and the LED.

The requirement of non-incompatibility is not self-evident. This showed during the difficult discussions during the legislative process of the new regulatory framework about the derogations of the requirement.[869] Regardless of frequently being put in a position to do so, the CJEU has not yet pointed to an interference with fundamental rights when data is processed for incompatible purposes.[870] Two derogations from the requirement are possible.

***Lex specialis*-derogation** The first derogation that can be made to the non-incompatibility requirement concerns re-use of data based on a *lex specialis* rule as permitted in art. 6(4) GDPR.[871] The *lex specialis* must meet the justification criteria stemming from the fundamental rights law. The derogation must pursue a legitimate aim, which are exhaustively listed in art. 23(1) GDPR. The derogation must also be provided for by law, and must be necessary in a democratic society. When considering the foreseeability, the re-use in relation to the original purposes must be taken into account. For this reason, this derogation is still linked to the initial purposes at the time of data collection. As soon as the intended re-use meets these criteria, the data can be re-used. The

[866] Summary based on Section 5.1.1 of this study.
[867] Summary based on Section 5.1.3 of this study.
[868] Summary based on Section 5.1.1.3 of this study.
[869] Summary based on Section 5.1.2.1 of this study.
[870] Summary based on Section 5.1.2.2 of this study.
[871] Summary based on Section 5.2 of this study.

new processing must be based on the processing ground of art. 6(1)(c) GDPR: a legal provision. The re-use is considered as a new processing procedure, which must meet the four cumulative criteria of data protection law. For this new processing procedure, use limitation is based on the compatibility of the purposes of further processing with the purpose at the time of the first re-use.

***Renewed consent* derogation** The second derogation concerns re-use after the data subject gave *renewed consent* for the processing for the new purposes.[872] This type of re-use grants the data controller the most liberty because there is no connection or assessment with the purposes at the time of data collection. The new processing is based on the processing ground in art. 6(1)(a) GDPR: consent. Again, as soon as lawful consent has been granted, the processing procedure for the new purposes must independently meet the four cumulative criteria for the lawfulness of the data processing.

Further processing on the basis of Recital 50 and art. 6(1)(f) GDPR

For a moment during the legislative process of the new regulatory framework a special provision was proposed which would have regulated access by competent authorities to data not covered by the LED.[873] In the end, this provision was not adopted. The European legislature deemed the back and forth references in the GDPR and the LED to adequately cover the lawfulness of the data transfers. These back and forth references have, however, a much broader scope than the specific provision that was temporarily proposed.

Recital 50 GDPR is intended to provide guidance on voluntary data transfers for the detection of criminal offenses between private entities and competent authorities:

> *Indicating possible criminal acts or threats to public security by the controller and transmitting the relevant personal data in individual cases or in several cases relating to the same criminal act or threats to public security to a competent authority should be regarded as being in the legitimate interest pursued by the controller.*

[872] Summary based on Section 5.3 of this study.
[873] Summary based on Section 5.4.2 of this study.

This recital only applies to a certain type of data transfer. First, the data must relate to *individual cases or in several cases relating to the same criminal act*. This means that *ad hoc* data transfers are covered, but more structural partnerships where the competent authorities have direct access to the databases of the responsible person are not. Secondly, the data must point in the direction of possible criminal acts or threats to public security. This means that the transmission of bulk data is out of the scope of this recital. It is unclear whether Recital 50 GDPR includes the transmission of data that is selected because the data subjects concerned met a profile that gives a high indication of possible criminal behavior. On the one hand, such data may indicate possible criminal acts; on the other hand, such data will not relate to individual cases or different cases related to the same criminal act.

The last part of the sentence in Recital 50 GDPR refers to the legitimate interests of the data controller as the appropriate lawful processing ground, art. 6(1)(f) GDPR, also known as the f-ground:

> *Processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data[...].*.

When looking at the four cumulative criteria of data processing, Recital 50 GDPR only refers to the criteria of a lawful processing ground. The purpose limitation principle remains therefore fully applicable. This has two implications. Firstly, the data protection framework only allows two types of derogations from the non-incompatibility requirement: re-use on the base of a *lex specialis* ex art. 6(4) juncto 6(1)(c) GDPR or with the consent of the data subject ex art. 6(4) juncto 6(1)(a) GDPR. There is no derogation related to processing on base of the f-ground. This means that the transfer of personal data to competent authorities for the purpose of detection of crime must be specified at the time of the initial data collection or at the time of the first lawful re-use. In other words, the controller must have already foreseen the transmission and communicated its possibility with the data subjects. Secondly, the control of the private entity over the processing purposes after the transmission of the personal data is unclear. In the back and forth references in the GDPR and the LED, the European Commission underlined that, when a data transfer is based on a legal obligation to which the private entity must comply, the competent authorities can consider the

transfer as their 'initial processing operation'. In other words, the data is stripped of its initial purpose. The European Commission is silent on the expiry of the initial purpose when data is voluntarily transmitted.

Use limitation based on the justification criteria stemming from fundamental rights law

Contrary to the GDPR, the LED only knows one derogation from the requirement of non-incompatibility. Pursuant to art. 4(2) LED, data may be processed for incompatible purposes if the data controller is authorized to process the data for the new purpose, the processing serves a legitimate aim and the processing is necessary and proportionate.[874] These criteria are well-known because fundamental rights law imposes the same obligations on the data controller when the processing falls under the scope of art. 8 ECHR. In almost all cases of processing of personal data for objectives of criminal law enforcement, the competent authorities have to comply with these fundamental right requirements, because the mere processing of personal data for criminal law enforcement objectives infringes the right protected by the first paragraph of art. 8 ECHR. The case law shows that the question on whether data is processed for an initial or a new purpose is not relevant for the determination of an interference with art. 8(1) ECHR and, subsequently, it is not relevant for the application of the criteria of the second paragraph of art. 8 ECHR: legitimate aim, legality and proportionality.

This gives the requirement of non-compatibility a much smaller role in the limitation of processing within the field of criminal law enforcement. because it is already common practice for a competent authority to meet these criteria that are now imposed because the data is processed for incompatible purposes. The law does not create an additional hurdle to process the data for an incompatible purpose. As a result the default use limitation under the LED is changed from use limitation based on compatibility of purposes to use limitation based on the criteria stemming from fundamental rights law.

[874] Summary based on Section 5.5 of this study.

Use limitation by strict interpretations of the purpose specification

European data protection law provides for two forms of prescribed processing restrictions based on strict interpretations of the purpose specification.[875] Both can be found in the LED.

In the first form, the strict use limitation is stipulated by law and is linked to the exercise of the rights of the data subject. In cases where it is not entirely clear to the controller whether the request for e.g. deletion of the data originates from the data subject herself, the controller may ask the applicant for additional personal data to identify wether the applicant is the data subject. According to recital 41 LED, such additional information may only be processed for the specific purpose of identification and may not be stored longer than necessary for that purpose. Therefore, this type of information is not subject to use limitation based on compatibility of purposes or by the criteria for the protection of fundamental rights. Under the second form of strict use limitation, the purposes are determined by the controller transferring data to another controller. Under the LED, a competent authority can transfer data to third countries and international organizations when appropriate safeguards are put in place for the protection of personal data. The legislature suggested as safeguards confidentiality and the notion that data is not processed for purposes other than those for which the data is transferred. *Other purposes* is a stricter criterion than *incompatible purposes*, because new purposes can be different but still compatible with the initial purposes.

Conclusions

The results of this study indicate a hierarchy of data protection principles.[876] All data protection principles must be respected in order to ensure the lawfulness of the processing. However, when it comes to the non-incompatibility requirement of the purpose limitation principle, two derogations are legitimately allowed. These derogations are not bound to limited application, as is the case with restrictions to data protection principles. The data minimization, storage limitation, transparency and accuracy principles can be lawfully restricted in exceptional cases. For the purpose

[875] Summary based on Section 5.7 of this study.
[876] Summary based on Section 5.2.1 of this study.

specification requirement of the purpose limitation principle, the lawfulness and adequacy principle as well as the integrity and confidentiality principle, no restrictions or derogations are allowed because these principles are either secured in art. 8(2) CFREU or the CJEU has linked the principles to the essence of the fundamental right to the protection of personal data. The requirement of non-compatibility is brought into connection with the fundamental right to the protection of personal data by the CJEU.

The following conclusion can be drawn: the purpose limitation principle has two requirements with an entirely different status. The requirement of non-incompatibility knows two legal derogations to it, whereas the purpose specification requirement belongs to the essence of the fundamental right to the protection of personal data.

The derogation of the non-incompatibility requirement under the LED does not impose any additional processing restrictions on the data controller. On paper the default use limitation in the LED is based on compatibility of purposes. Nevertheless, in practice the default use limitation can be based on the derogation, and therefore, on the justification criteria stemming from fundamental rights law. In most cases the processing of competent authorities has to meet the justification criteria stemming from fundamental rights already because the processing falls under the scope of art. 8(1) ECHR. This shifts the default use limitation under the LED from use limitation based on compatibility to purposes to use limitation based on the criteria for the protection of fundamental rights.

Case law analysis shows that the purpose specification requirement is linked to all criteria for the protection of fundamental rights: the legitimate aim, legality and proportionality. The factors for the GDPR compatibility test are also all reflected in the case law of the ECtHR. By no means does the ECtHR apply a structured compatibility test, but the considerations affecting the factors of the test can be used to substantiate the compatibility test. Due to the autonomous and conditional function of the purpose specification principle, a change to the purpose limitation principle implies a change in the protection afforded by data protection law and the protection of fundamental rights. In addition to use limitation based on compatibility of purposes and use limitation based on the criteria for the protection of fundamental rights, European data protection law also provides use limitation based on privileged purposes, and use limitation based on strict interpretations of the purpose specification.

As regards voluntary data transfers from private entities to competent authorities for the detection of crime, the following conclusion can be drawn: These transfers are subjected to Recital 50 GDPR, which has a narrow scope of application. Recital 50 refers to the f-ground. For this lawful processing ground, no derogation exists with regard to the requirement of non-incompatibility. This means that the data must be collected for the purpose of transfer to competent authorities for the detection of crime. Recital 50 GDPR provides for the *ad hoc* transmission of data relating to a specific offense. The provision cannot be used for the sharing of bulk data. The legislature does not provide the same clarity for the lawfulness of personal data that is shared after it is being selected based on a profile. In determining liability for interferences or violations of fundamental rights in partnerships between private parties and competent authorities, the ECtHR uses criteria that differ from the criteria of data controller and data processor under the GDPR and the LED. This can result in a situation in which the private entity that transfers data to a competent authority should be considered the data controller under the GDPR, because the private party determines the purposes and means, but the competent authority can be held accountable for the data processing under the ECHR. Once the data has been transferred, the private party no longer controls the purposes of the processing. If the data has been unlawfully obtained by the private party, the lawfulness of the processing carried out by the competent authorities after a mandatory transmission is not affected. The law does not regulate the effect of unlawfully obtained data on the data processing of the competent authorities if it has later been voluntarily transmitted by the private party to a competent authority.

Based on these conclusions the European legislature is advised to clarify the framework on voluntary data transfers from private entities to criminal law enforcement authorities for the detection of crime with a focus on the protection of fundamental rights. Civil society is recommended to develop strategic litigation procedures based on the conclusions of this study in order to challenge the data broker industry that caters to criminal law enforcement for predictive policing purposes.

Samenvatting in het Nederlands

Dit onderzoek richt zich op het doelbindingsbeginsel, dat bepaalt dat persoonsgegevens enkel voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden mogen worden verzameld en dat deze gegevens niet verder worden verwerkt op een met die doeleinden onverenigbare wijze. Dit beginsel heeft twee poten: het doelspecificatievereiste en het vereiste van niet-onverenigbaarheid. Het vereiste van niet-onverenigbaarheid is een type verwerkingsbeperking. Voor dit onderzoek worden de twee vereisten onafhankelijk van elkaar onderzocht, waarbij wat betreft verwerkingsbeperking alle typen verwerkingsbeperking worden onderzocht die het gegevensbeschermingsrecht rijk is, inclusief het vereiste van niet-onverenigbaarheid. LEDDe resultaten worden voornamelijk gebaseerd op secundair onderzoek, waarbij de relevante bronnen van het recht worden doorgespit: wetgeving, jurisprudentie, doctrine, en opinies en richtlijnen van het Europees Comité voor gegevensbescherming en andere adviesorganen.

Aanleiding en centrale onderzoeksvraag

De aanleiding van dit onderzoek is tweeledig.[877]

Enerzijds is er toenemende kritiek op het doelbindingsbeginsel. Het beginsel wordt als achterhaald beschouwd en als moeilijk te rijmen met de data-gedreven

[877] Samenvatting gebaseerd op paragraaf 1.1 van dit onderzoek.

samenleving waarvan de toekomst ligt in *big data*-analyse en kunstmatige intelligentie. In de ontwerpbeslissingen van de laatste twee technologieën wordt op dit moment inderdaad weinig rekening gehouden met het juridisch bindende doelbindingsbeginsel voor de verantwoordelijke voor de inzet van de technologie op de Europese markt.

Anderzijds is het gebruik van algoritmische voorspellingsmodellen in combinatie met *big data*-analyse, zoals profilering, in opkomst binnen de strafrechtelijke opsporingsketen. Zogeheten *predictive policing* systemen worden ontwikkeld voor en door opsporingsdiensten. Deze systemen analyseren (bulk) gegevenssets voor de detectie van strafbare feiten in de vroegsporingsfase van de strafvordering. Het gevaar ligt op de loer dat de input voor deze systemen zal bestaan uit (bulk) gegevens die door commerciële partijen zijn verzameld voor een ander doel dan de detectie van strafbare feiten. Dit levert spanning op met het doelbindingsbeginsel.

Sommige wetenschappers hebben voorgesteld om het doelbindingsbeginsel te vervangen door een systeem dat uitgaat van de belangen van de verantwoordelijke bij de gegevensverwerking; in plaats van de doelen van de verwerking staan dan de belangen van de verantwoordelijke voor de gegevensverwerking centraal in de afwegingen omtrent verwerkingsbeperking. Alvorens te zoeken naar een alternatief voor het doelbindingsbeginsel, is het zaak om goed te begrijpen of, en zo ja waarvoor, een alternatief moet worden gezocht. Deze studie richt zich daarom op het doel en de beperkingen van het doelbindingsbeginsel.

De centrale onderzoeksvraag is dan ook:

> *Wat is de rol van het doelbindingsbeginsel in het Europees gegevensbeschermingsrecht en in de bescherming van fundamentele rechten?*

Relevant juridisch kader

Op het niveau van bescherming van de fundamentele rechten zijn voor dit onderzoek hoofdzakelijk van belang art. 8 van het Europees Verdrag voor de Rechten van de Mens (EVRM) en art. 7 en 8 van Handvest van de Grondrechten van de Europese Unie (Hv).

Het Europees Hof voor de Rechten van de Mens (EHRM) hanteert het begrip

gegevens gerelateerd aan het privéleven om in zaken te oordelen die onder het gegevensbeschermingsrecht vallen en een inmenging vormen op het eerste lid van art. 8 EVRM.[878] Bij de kwalificatie *gegevens gerelateerd aan het privéleven* spelen drie factoren een rol. Ten eerste, de bijzondere juridische status van de gegevens. Dit kan de status als bijzondere persoonsgegevens zijn, zoal bijvoorbeeld gezondheidsgegevens of gegevens over iemands etniciteit, en de status van gegevens over strafrechtelijke veroordelingen of -feiten. Ten tweede speelt het type gegeven mee. Zo zijn locatiegegevens, DNA-gegevens, portretten, communicatiegegevens en financiële gegevens door het EHRM al meerdere malen onder de reikwijdte van art. 8(1) EVRM gebracht. De derde factor die een rol speelt is het type gegevensverwerking. Voorbeelden van deze factor zijn het monitoren van gedrag en het opstellen van persoonsprofielen. Uit de jurisprudentie van het EHRM blijkt dat het instellen van gegevensbeschermingswaarborgen geen invloed heeft op de uitkomst van de vraag of een bepaalde gegevensverwerking onder het eerste lid van art. 8 EVRM valt.[879]

Slechts een enkele keer heeft het EHRM zich moeten buigen over een zaak waarbij de inmenging op het eerste lid van art. 8 EVRM door een private partij was begaan die niet in opdracht maar in samenwerking werkte met opsporingsautoriteiten.[880] In die zaken nam het EHRM de volgende aspecten in overweging: de duur van de samenwerking, de inbreng van de overheid, het belang van de opsporingsautoriteiten bij de inmenging en de controle die de autoriteiten uitoefende over de beslissingen en handelingen van de private partij. Inmenging op het eerste lid van art. 8 EVRM moet voloen aan de cumulatieve vereisten uit het tweede lid om te kunnen worden gerechtvaardigd onder het verdrag. De inmenging moet een legitiem doel nastreven, moet zijn voorzien bij wet, en moet noodzakelijk zijn in een democratische samenleving.

Het Handvest is van toepassing op wetgevings- en uitvoeringshandelingen van de instellingen, organen en instanties van de EU en op handelingen van de lidstaten wanneer zij EU-recht ten uitvoer brengen, bij de uitoefening van hun bevoegdheden.[881] De inwerkingtreding van het Verdrag van Lissabon in 2009 heeft drie dingen veranderd binnen het Europees gegevensbeschermingsrecht. In de eerste plaats is er nu een fundamenteel recht op bescherming van persoonsgegevens, zoals neergelegd in art. 8 Hv, dat onafhankelijk functioneert van het recht op privéleven ex art. 7 Hv.

[878] Samenvatting gebaseerd op paragraaf 2.1.1.2 van dit onderzoek.
[879] Samenvatting gebaseerd op paragraaf 2.1.1.3 van dit onderzoek.
[880] Samenvatting gebaseerd op paragraaf 2.1.1.4 van dit onderzoek.
[881] Samenvatting gebaseerd op paragraaf 2.1.2 van dit onderzoek.

Ten tweede is de rol van het Hof van Justitie van de Europese Unie (HvJEU) veranderd omdat dit Hof expliciet de taak erbij heeft gekregen om toe te zien op de naleving van de grondrechten in de EU. Ten derde is de reikwijdte van het Europees gegevensbeschermingsrecht vergroot. Hieronder valt nu ook verwerking van persoonsgegevens door bevoegde autoriteiten met het oog op de voorkoming, het onderzoek, de opsporing of de vervolging van strafbare feiten of de tenuitvoerlegging van straffen, met inbegrip van de bescherming tegen en de voorkoming van gevaren voor de openbare veiligheid.

Artikel 7 Hv legt het recht op bescherming voor het privéleven vast en is qua tekst en reikwijdte vrijwel gelijk aan art. 8 EVRM. Het eerste lid van art. 8 Hv waarborgt het fundamenteel recht op bescherming van persoonsgegevens. Dit recht is verder gespecificeerd in het tweede en derde lid van art. 8 Hv. Artikel 8(2) Hv omschrijft twee rechten voor de betrokkene van de gegevensverwerking: het recht op toegang tot de gegevens en het recht op rectificatie van de gegevens. Het lid legt ook drie voorwaarden neer voor de verwerking van persoonsgegevens: de gegevens moeten eerlijk worden verwerkt, voor bepaalde doeleinden en met toestemming van de betrokkene of op basis van een andere gerechtvaardigde grondslag waarin de wet voorziet. Deze voorwaarden zijn verbonden aan de volgende gegevensbeschermingsbeginselen: het doelspecificatievereiste van het doelbindingsbeginsel, het eerlijkheidsbeginsel en het rechtmatigheidsbeginsel. Het derde lid legt ook de waarborg neer van onafhankelijk toezicht op de naleving van het gegevensbeschermingsrecht. Uit de jurisprudentie lijkt een lijn zichtbaar te worden waarin het HvJEU de rechten uit artikel 7 en 8 Hv in samenhang toepast als *het recht op eerbiediging van het privéleven met betrekking tot de verwerking van persoonsgegevens*.

Het relevante gegevensbeschermingsrecht bestaat uit de herziene versie van het Gegevensbeschermingsverdrag uit 2016 (Gbv), Aanbeveling (87) 15 voor de regulering van het gebruik van persoonsgegevens in de politiesector (A (87) 15), de Algemene verordening gegevensbescherming (Avg) en de Richtlijn gegevensbescherming voor politiezaken (Rgp).

Algemeen idee achter het doelbindingsbeginsel

Doelbinding hakt gegevensverwerking op tot processen met een duidelijk begin- en eindpunt.[882] De verwerking moet worden ingericht op het behalen van de verwerkingsdoelen. Zodra het doeleinde is behaald vervalt de rechtmatigheid van de verwerking. Het doelbindingsbeginsel wordt door verschillende wetenschappers verschillende rollen toebedeeld. Die rollen zien toe op de transparantie, rechtszekerheid, verdeling van macht, integriteit, waardigheid, gelijkheid, autonomie, informationele zelfbeschikking, ondersteuning van de democratie, en een eerlijk proces.[883] Door deze rollen wordt aangenomen dat het doelbindingsbeginsel als een waarborg functioneert in verticale en horizontale verhoudingen tussen de verantwoordelijke en de betrokkenen. Het beginsel heeft een zestal relevante elementen.[884]

Ten eerste is het element van een *verwerkingsdoeleinde*, kortweg een *doeleinde* of *doel*, relevant. Het doeleinde is meestal het antwoord op de vraag: "Waarom worden hier persoonsgegevens verwerkt?". Deze vraag gaat vaak samen op met de vraag: "Hoe worden de persoonsgegevens verwerkt?", welke toeziet op de verwerkingsmiddelen. De verwerkingsdoeleinden moeten helder genoeg zijn om beslissingen te ondersteunen over de evenredigheid van de gegevensverwerking. Bij voorkeur worden de doeleinden vastgesteld in een schriftelijke doelspecificatie, zodat deze kunnen worden gecommuniceerd naar alle betrokken partijen, waaronder de toezichthoudende autoriteit.

Ten tweede speelt het element van een *gerechtvaardigd doeleinde* een rol. Een gerechtvaardigd doeleinde is een zelfstandig begrip dat verder gaat dan een rechtmatigheidstoets van de verwerking. De verwerkingsdoeleinden moeten overeenstemmen met de vereisten van het criterium *voorzien bij wet*, de verwerking moet overeenstemmen met *state of the art* technologie en sociale en culturele normen. De verantwoordelijkheid voor de gerechtvaardigheid van de doeleinden ligt bij verwerkingsverantwoordelijke.

Het derde element is de *welbepaaldheid* van het doeleinde. Dit houdt in dat de gerechtvaardigde doeleinden precies en volledig moeten worden gearticuleerd zodat iedere betrokkene, ook die zonder juridische- of technische kennis, kan inschatten

[882] Samenvatting gebaseerd op paragraaf 3.1 van dit onderzoek.
[883] Samenvatting gebaseerd op paragraaf 3.4 van dit onderzoek.
[884] Samenvatting gebaseerd op paragraaf 3.3 van dit onderzoek.

welke verwerking er wel en welke verwerking niet onder de verwerkingsprocedure valt. Binnen het Engelstalige wetenschappelijke veld is onduidelijkheid ontstaan of het *welbepaalde doeleinde* toeziet op *gespecificeerde doelen* of op *specifieke doelen*. Het ontbreekt gespecificeerde doelen echter aan normstelling, waardoor de communicatiefunctie van het criterium *welbepaalde doeleinde* niet kan worden uitgeoefend en de doeleinden niet kunnen dienen als factor in andere evenredigheidsbeslissingen die binnen het gegevensbeschermingsrecht gemaakt moeten worden. Het criterium *welbepaalde doeleinden* komt hierdoor dichterbij specifieke doelen dan bij gespecificeerde doelen. De enige uitzondering die is gemaakt binnen het gegevensbeschermingsrecht op de eis van welbepaalde doelen is voor de verwerking van persoonsgegevens voor wetenschappelijke doeleinden. Onder de Avg moeten betrokkenen in de gelegenheid kunnen worden gesteld om toestemming te verlenen voor de verwerking van hun persoonsgegevens binnen bepaalde velden van wetenschappelijk onderzoek, zonder dat het specifieke doel op voorhand is vastgesteld.

Ten vierde moeten de doeleinden *uitdrukkelijk worden omschreven*. Dit element komt alleen voor binnen het EU-recht. De doeleinden moeten duidelijk kenbaar worden gemaakt zodat alle partijen een unaniem idee kunnen vormen over de te verwachten gegevensverwerking. Bij voorkeur worden de doelen neergelegd in een schriftelijke doelspecificatie.

Timing is van belang voor het doelbindingsbeginsel en is het vijfde element. De doeleinden moeten namelijk voorafgaand aan de aanvang van de gegevensverwerking worden gespecificeerd.

Het laatste element betreft *verenigbaarheid* van het initiële doel bij gegevensverzameling met de doelen van verdere verwerking. Dit element is direct aan het vereiste van niet-onverenigbaarheid verbonden en wordt getoetst door te kijken naar:

- Elk verband tussen de doeleinden waarvoor de persoonsgegevens zijn verzameld en de doeleinden van de beoogde verdere verwerking.

- De context waarin de persoonsgegevens zijn verzameld, met name wat betreft de relatie tussen de betrokkenen en de voor de verwerking verantwoordelijke en met inbegrip van de redelijke verwachtingen van de betrokkenen op basis van hun relatie met de voor de verwerking verantwoordelijke wat betreft het verdere gebruik van de gegevens.

- De aard van de persoonsgegevens, in het bijzonder of er speciale categorieën van persoonsgegevens worden verwerkt, of dat er persoonsgegevens in verband met strafrechtelijke veroordelingen worden verwerkt.
- De mogelijke gevolgen van de voorgenomen verdere verwerking voor de betrokkenen.
- Het bestaan van passende waarborgen bij zowel de oorspronkelijke als de voorgenomen verdere verwerking, die versleuteling of pseudonimisering kunnen omvatten.

Gegevensverwerking moet aan vier voorwaarden voldoen om rechtmatig te zijn onder het Europees gegevensbeschermingsrecht.[885]

In de eerste plaats moet de verwerking aan de gegevensbeschermingsbeginselen voldoen, waaronder ook het doelbindingsbeginsel. Ten tweede moet de verwerking zijn gestoeld op een van de rechtmatige verwerkingsgronden. Ten derde moet de verwerkingsverantwoordelijke aan de verplichtingen voor de verantwoordelijke voldoen. Als laatste moeten de betrokkenen in staat worden gesteld om hun rechten uit te oefenen. Deze voorwaarden zijn cumulatief, waardoor over het algemeen geldt dat het doelbindingsbeginsel niet aan de kant kan worden geschoven als de verantwoordelijke de verdere verwerking baseert op een nieuwe rechtmatige verwerkingsgrond. Op deze regel van cumulatie zijn twee uitzonderingen die verderop in deze samenvatting worden besproken.

Het doelspecificatievereiste

Het doelspecificatievereiste heeft twee functies.[886] Een autonome functie die terugslaat op het beginsel zoals in de voorgaande alinea's is omschreven, en een conditionele functie, waarbij het vereiste direct of indirect van invloed is op de toepasbaarheid, toepassing en uitkomst van andere regels binnen het gegevensbeschermingsrecht. Directe afhankelijkheid betekent afhankelijkheid van het vereiste en de status die het vereiste heeft binnen het gegevensbeschermingsrecht als poot van een prominent gegevensbeschermingsbeginsel: het doelbindingsbeginsel. De gegevensbescher-

[885] Samenvatting gebaseerd op paragraaf 3.5 van dit onderzoek.
[886] Samenvatting gebaseerd op paragraaf 4.1 van dit onderzoek.

mingsbeginselen hebben directe afhankelijkheid van het doelspecificatievereiste omdat zij gezamenlijk een sluitend raamwerk van bescherming vormen.[887]

Indirecte afhankelijkheid slaat op de afhankelijkheid van andere regels uit het gegevensbeschermingsrecht op de verwerkingsdoeleinden of op de doelspecificatie. Deze indirecte afhankelijkheid bestaat er voor de toebedeling van rollen binnen het gegevensbeschermingsrecht, waaronder de rol van verwerkingsverantwoordelijke, verwerker, ontvanger en de bevoegde leidende toezichthoudende autoriteit.[888] De conditionele functie van het doelspecificatievereiste strekt zich ook uit tot de toepassing van de rechtmatige verwerkingsgronden omdat deze afhankelijk zijn van de verwerkingsdoeleinden en in voorkomend geval de doelspecificatie zelf.[889] De verwerkingsdoeleinden bepalen ook de toepassing en uitkomst van een beroep op het recht op gegevenswissing, het recht van bezwaar, en het recht niet te worden onderworpen aan een uitsluitend op geautomatiseerde verwerking gebaseerd besluit dat rechtsgevolgen heeft of dat de betrokkene anderszins in aanmerkelijke mate treft.[890] Met de inwerkingtreding van het nieuw regelgevend kader in de EU in 2016 is de conditionele functie uitgebreid. De verantwoordelijkheden waaraan de verwerkingsverantwoordelijke moet voldoen zijn in toenemende mate afhankelijk van de verwerkingsdoelen.[891] Hieronder vallen de verplichting tot gegevensbescherming door ontwerp en door standaardinstellingen, het uitvoeren van een gegevensbeschermingseffectbeoordeling, de beveiliging van de verwerking, en het aanwijzen van een vertegenwoordiger in de EU en van een Functionaris voor gegevensbescherming. De doeleinden bepalen ook of de verwerking in aanmerking komt voor het speciale regime voor gegevensverwerking voor geprivilegieerde doeleinden met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden.[892] Het karakter van de handhaving en de proportionaliteitsafweging bij de handhaving door de toezichthoudende autoriteit is afhankelijk van de verwerkingsdoeleinden en de doelspecificatie die al dan niet is opgesteld door de verwerkingsverantwoordelijke.[893]

In eerste oogopslag lijkt het EHRM in zijn uitspraken niet te refereren aan het doelbindingsbeginsel. Toch is het beginsel alom doch subtiel vertegenwoordigd in

[887] Samenvatting gebaseerd op paragraaf 4.1.3 van dit onderzoek.
[888] Samenvatting gebaseerd op paragraaf 4.1.1 van dit onderzoek.
[889] Samenvatting gebaseerd op paragraaf 4.1.2 van dit onderzoek.
[890] Samenvatting gebaseerd op paragraaf 4.1.4 van dit onderzoek.
[891] Samenvatting gebaseerd op paragraaf 4.1.5 van dit onderzoek.
[892] Samenvatting gebaseerd op paragraaf 4.1.5.5 van dit onderzoek.
[893] Samenvatting gebaseerd op paragraaf 4.1.6 van dit onderzoek.

de afweging rondom de aanwezigheid en het gewicht van een inmenging op het eerste lid van art. 8 EVRM.[894] Daarnaast besteden zowel het HvJEU en het EHRM aandacht aan het doelspecificatievereiste bij de toetsing van de drie rechtvaardigingscriteria van het tweede lid van art. 7 en 8 Hv en/of art. 8 EVRM. Het legitiem doel dat met een inmenging wordt nagestreefd is een ander concept dan het verwerkingsdoeleinde. Maar het laatste vormt in veel gevallen wel het startpunt van de bepaling van het legitieme doel bij de verwerking van gegevens gerelateerd aan het privéleven.[895] Het criterium voorzien bij wet beslaat de kwaliteit van de wet, waaronder de toegankelijkheid en voorzienbaarheid van een inmenging. De doelspecificatie speelt hier een belangrijke rol in.[896] Het doelspecificatievereiste is voorwaardelijk voor de evenredigheidsafweging die gepaard gaat met de toepassing van het criterium: noodzakelijkheid in een democratische samenleving in zaken over de verwerking van gegevens gerelateerd aan het privéleven.[897] Een onverwachte uitkomst van het onderzoek naar het doelbindingsbeginsel is dat het doelspecificatievereiste vanwege de autonome en conditionele functie binnen het gegevensbeschermingsrecht en de bescherming van fundamentele rechten tot de kern van het fundamenteel recht op bescherming van persoonsgegevens behoort.[898] Hierdoor kan dit vereiste onder geen beding worden beperkt. De beperking van het doelspecificatievereiste is een ontoelaatbare inmenging op het recht op bescherming van persoonsgegevens.[899]

Verwerkingsbeperking

Het gegevensbeschermingsrecht kent verschillende vormen van verwerkingsbeperking die hieronder worden samengevat.

Verwerkingsbeperking door verenigbaarheid van doeleinden

Het meest bekende type verwerkingsbeperking is beperking op basis van de verenigbaarheid van de doeleinden van verdere verwerking met de doeleinden op het mo-

[894] Samenvatting gebaseerd op paragraaf 4.2 van dit onderzoek.
[895] Samenvatting gebaseerd op paragraaf 4.2.1 van dit onderzoek.
[896] Samenvatting gebaseerd op paragraaf 4.2.2 van dit onderzoek.
[897] Samenvatting gebaseerd op paragraaf 4.2.3 van dit onderzoek.
[898] Samenvatting gebaseerd op paragraaf 4.2.4 van dit onderzoek.
[899] Samenvatting gebaseerd op paragraaf 4.3 van dit onderzoek.

ment van de verzameling van de gegevens. Deze vorm van beperking is direct verbonden aan het vereiste van niet-onverenigbaarheid van het doelbindingsbeginsel. Dit type verwerkingsbeperking dwingt een verenigbaarheidstest af.[900] In deze test moeten de doeleinden aan de criteria worden getoetst die zijn opgesomd op bladzijde 240 als de gegevensverwerking onder de Avg valt. Deze criteria zijn allemaal ook los terug te vinden in de redeneringen van het EHRM in zaken die gingen over verdere verwerking van gegevens gerelateerd aan het privéleven.[901] Deze jurisprudentie kan gebruikt worden om de criteria verder in te vullen. De Rgp legt enkel verwerkingsbeperking door verenigbaarheid van doeleinden neer door het waarborgen van het vereiste van niet-onverenigbaarheid.[902] Verdere uitleg ontbreekt over de toepassing van dit vereiste voor gegevensverwerking die onder de reikwijdte van de Rgp valt. Deze uitleg ontbreekt ook in het Gbv dat van toepassing is op gegevensverwerking die valt onder de Avg en onder de Rgp.

Het vereiste van niet-onverenigbaarheid is niet vanzelfsprekend. Dit blijkt uit de moeizame discussie tijdens het wetgevend proces van het nieuwe regelgevend kader over de afwijkingen die op het vereiste zouden worden toegestaan.[903] Ook is het HvJEU niet happig op het duiden van een inmenging op de grondrechten door een afwijking van de regel van verwerkingsbeperking door verenigbaarheid van doelen.[904] Het HvJEU is hier wel meermaals toe in de gelegenheid gesteld.

Afwijkingen van de beperking door verenigbaarheid van doeleinden

Het is een veelvoorkomende misvatting dat het vereiste van niet-onverenigbaarheid kan worden beperkt. Dit is niet mogelijk omdat de beperkingsclausule van de Avg, art. 23(1), hier niet in voorziet. Deze clausule voorziet wel in de beperking van het minimale gegevensverwerking-, opslagbeperking-, transparantie-, en juistheidbeginsel. De gegevensverwerkingsbeginselen die niet kunnen worden beperkt zijn: het doelspecificatievereiste van het doelbindingsbeginsel, het rechtmatigheids- en behoorlijkheidsbeginsel, en het integriteits- en vertrouwelijkheidsbeginsel. Deze "beperkingsbeperking" vloeit voort uit de speciale status van deze beginselen in het

[900] Samenvatting gebaseerd op paragraaf 5.1.1 van dit onderzoek.
[901] Samenvatting gebaseerd op paragraaf 5.1.3 van dit onderzoek.
[902] Samenvatting gebaseerd op paragraaf 5.1.1.3 van dit onderzoek.
[903] Samenvatting gebaseerd op paragraaf 5.1.2.1 van dit onderzoek.
[904] Samenvatting gebaseerd op paragraaf 5.1.2.2 van dit onderzoek.

tweede lid van art. 8 Hv of omdat het HvJEU de beginselen in verband heeft gebracht met de kern van het fundamenteel recht op bescherming van persoonsgegevens. Zoals al reeds gesteld kan het vereiste van niet-onverenigbaarheid ook niet worden beperkt onder art. 23(1) Avg. Er zijn echter wel twee afwijkingen toegestaan op dit vereiste waarbij verdere verwerking is toegestaan ondanks onverenigbaarheid van de doeleinden van verdere verwerking met de doeleinden op het moment van de verzameling van de gegevens.

***Lex specialis*-afwijking** De eerste afwijking betreft hergebruik van gegevens gebaseerd op een *lex specialis* regel zoals toegestaan in art. 6(4) Avg.[905] De *lex specialis* moet voldoen aan de rechtvaardigingscriteria die voortvloeien uit de bescherming van fundamentele rechten. De afwijking moet een legitiem doel nastreven. Voor de vaststelling van deze doelen wordt verwezen naar art. 23(1) Avg. De afwijking moet ook zijn voorzien bij wet, en moet noodzakelijk zijn in een democratische samenleving. Bij de afweging van de voorzienbaarheid moet het hergebruik in relatie tot de oorspronkelijke doeleinden worden meegewogen. Bij deze afwijking is er daarom nog altijd een verbinding met de doeleinden op het moment van de gegevensverzameling. Zodra de afwijking aan deze criteria voldoet, kunnen de gegevens worden hergebruikt. De nieuwe verwerking moet worden gestoeld op de verwerkingsgrond uit art. 6(1)(c) Avg: een wettelijke bepaling. Het hergebruik wordt als een nieuwe verwerkinsgprocedure beschouwd, die aan de vier cumulatieve voorwaarden van het gegevensbeschermingsrecht moeten voldoen. Voor deze nieuwe verwerkingsprocedure geldt dat de verwerkingsbeperking is gestoeld op de verenigbaarheid van de doeleinden van verdere verwerking met de doeleinden op het moment van het eerste hergebruik.

***Hernieuwde toestemming*-afwijking** De tweede afwijking betreft hergebruik na *hernieuwde toestemming* van de betrokkenen.[906] Bij dit type hergebruik heeft de verwerkingsverantwoordelijke de meeste vrijheid en is er geen verbinding met de doeleinden op het moment van de gegevensverzameling. De nieuwe verwerking is gestoeld op de verwerkingsgrond uit art. 6(1)(a) Avg: toestemming. Ook hier geldt dat, zodra rechtmatige toestemming is verleend, de verwerkingsprocedure voor de

[905] Samenvatting gebaseerd op paragraaf 5.2 van dit onderzoek.
[906] Samenvatting gebaseerd op paragraaf 5.3 van dit onderzoek.

nieuwe doeleinden zelfstandig moet voldoen aan vier cumulatieve voorwaarden voor de rechtmatigheid van de gegevensverwerking.

Verdere verwerking op basis van Recital 50 en art. 6(1)(f) Avg

Tijdens het wetgevend proces van het nieuw regulerend raamwerk was er even sprake van een speciale bepaling die toegang regelde voor bevoegde autoriteiten tot gegevens die niet onder de Rgp vallen.[907] Uiteindelijk is niet voor een speciale bepaling gekozen en heeft de Europese wetgever aangegeven dat de heen-en-weer-verwijzingen in de Avg en de Rgp afdoende de gegevensverwerkingsrisico's afdekken omdat er altijd een instument van toepassing is. Toch hebben de heen-en-weer-verwijzingen in beide instrumenten een veel bredere reikwijdte dan de tijdelijk voorgestelde specifieke bepaling.

Recital 50 Avg moet houvast bieden aan vrijwillige gegevensoverdracht voor de detectie van strafbare feiten tussen private partijen en bevoegde autoriteiten:

> *Het aanwijzen van mogelijke strafbare feiten of gevaren voor de openbare veiligheid door de verwerkingsverantwoordelijke en de doorzending van de desbetreffende persoonsgegevens in individuele zaken of in verschillende zaken die met hetzelfde strafbare feit of dezelfde gevaren voor de openbare veiligheid te maken hebben, aan een bevoegde instantie moeten worden beschouwd als zijnde in het gerechtvaardigde belang van de verwerkingsverantwoordelijke.*

Recital 50 is slechts van toepassing op een bepaald type gegevensoverdracht. Ten eerste moeten de gegevens relateren aan *individuele zaken of in verschillende zaken die met hetzelfde strafbare feit of dezelfde gevaren voor de openbare veiligheid*. Dit betekent dat *ad hoc* data transfers hier wel onder vallen, maar meer structurele samenwerkingsverbanden hier niet onder vallen waarbij de bevoegde autoriteiten directe toegang tot de databanken van de verantwoordelijke krijgen. Ten tweede moeten de gegevens in de richting van mogelijke strafbare feiten of gevaren voor de openbare veiligheid wijzen. Dat betekent dat de doorzending van bulkgegevens buiten de reikwijdte valt. Het is onduidelijk of Recital 50 ook voorziet in de doorzending van gegevens die worden doorgezonden omdat de betreffende betrokkene aan een profiel voldoet dat een hoge indicatie geeft van mogelijk strafbaar gedrag. Enerzijds kunnen

[907] Samenvatting gebaseerd op paragraaf 5.4.2 van dit onderzoek.

die gegevens mogelijke strafbare feiten aanwijzen; anderzijds zullen die gegevens geen verband houden met individuele zaken of verschillende zaken die relateren aan hetzelfde strafbare feit.

Het laatste deel van de zin uit Recital 50 Avg refereert aan de gerechtvaardigde belangen van de verwerkingsverantwoordelijke en daarmee ook naar de verwerkingsgrond art. 6(1)(f) Avg (de f-grond):

> *De verwerking is noodzakelijk voor de behartiging van de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of van een derde, behalve wanneer de belangen of de grondrechten en de fundamentele vrijheden van de betrokkene die tot bescherming van persoonsgegevens nopen, zwaarder wegen dan die belangen [...].*

Recital 50 refereert alleen aan een verwerkingsgrond; het doelbindingsbeginsel blijft hierdoor onverminderd van toepassing. Dit heeft twee implicaties. Ten eerste speelt de regel van cumulatieve verwerkingsvoorwaarden een rol. Zoals op bladzijde 244 aangegeven, bestaan er twee mogelijkheden om gegevens in afwijking met het vereiste van niet-overeenigbaarheid te kunnen verwerken: op basis van een *lex specialis* ex art. 6(4) juncto 6(1)(c) Avg of met toestemming van de betrokkenen ex art. 6(4) juncto 6(1)(a) Avg. De Avg voorziet niet een dergelijke afwijking voor verwerking die op de f-grond is gebaseerd. Dit betekent dat doorzending van persoonsgegevens naar bevoegde autoriteiten voor het aanwijzen van mogelijke strafbare feiten bij de initiële verwerkingsdoeleinden moet horen. Met andere woorden: de verwerkingsverantwoordelijke moet de doorzending al hebben voorzien en de mogelijkheid daarvan hebben gecommuniceerd aan de betrokkenen.

Ten tweede is het de vraag in hoeverre de doorzendende partij invloed heeft op de verdere verwerking van de gegevens door de bevoegde autoriteiten. In het heen-en-weer-verwijs tussen de Avg en de Rgp heeft de Europese Commissie aangegeven dat, voorzover de doorzending is gestoeld op een wettelijke plicht waar de verantwoordelijke gehoor aan moet geven, de bevoegde autoriteiten het ontvangen van de gegevens als een initiële verwerking kunnen beschouwen. Met andere woorden: het verwerkingsdoeleinde dat de verantwoordelijke nastreefde voorafgaand aan de confrontatie met de wettelijke plicht tot doorzending van de gegevens, doet er niet toe voor de autoriteiten. Zij beginnen met een schone lei. Over het vervallen van het

oorspronkelijk doeleinde wanneer gegevens vrijwillig zijn doorgezonden, heeft de Europese Commissie niets gezegd. Een van de aanleidingen van dit onderzoek is de opkomst van *predictive policing* systemen die gebruik maken van vrijwillig verstrekte gegevens. Over de doelbinding van vrijwillig toegezonden gegevens zegt de Europese wetgever niets.

Verwerkingsbeperking door toepassing van de criteria voor de bescherming van fundamentele rechten

De Rgp kent in tegenstelling tot de Avg, maar een afwijkingsmogelijkheid van het vereiste van niet-onverenigbaarheid. Ingevolge art. 4(2) Rgp kunnen gegevens voor onverenigbare doelen worden verwerkt indien de verantwoordelijke gemachtigd is om de gegevens voor het doel te verwerken, dit een legitiem doel dient en de verwerking noodzakelijk en proportioneel is.[908] Deze criteria komen bekend voor omdat dit dezelfde verplichtingen zijn, als die al rusten op het bevoegde gezag vanuit het raamwerk ter bescherming van fundamentele rechten. Daarnaast moeten de bevoegde autoriteiten in bijna alle gevallen van persoonsgegevensverwerking voor doeleinden binnen de strafvordering aan deze eisen uit het fundamenteel recht voldoen, omdat het enkele verwerken van persoonsgegevens voor strafvorderlijke doeleinden inmengt op het recht dat is beschermd in het eerste lid van art. 8 EVRM. Uit de jurisprudentie blijkt dat de vraag of de gegevens worden verwerkt voor een initieel of nieuw doel niet van belang is voor de vaststelling van de inmenging op art. 8(1) EVRM en daarmee de toepassing van de criteria uit het tweede lid van art. 8 EVRM: legitiem doel, voorzien bij wet of noodzakelijkheid in een democratische samenleving. Hierdoor krijgt het vereiste van niet-onverenigbaarheid een veel kleinere rol in de verwerkingsbeperking binnen de strafvordering. Het is namelijk de normale gang van zaken om als bevoegde autoriteit aan de criteria te voldoen waar aan voldaan zou moet worden wanneer de gegevens voor een onverenigbaar doeleinde worden verwerkt. Er wordt door het recht niet een extra hindernis opgeworpen die genomen moet worden om de gegevens voor een onverenigbaar doel te verwerken. Hierdoor verandert, in mijn ogen, de standaard verwerkingsbeperking binnen de strafvordering van verwerkingsbeperking door verenigbaarheid van doeleinden naar verwerkingsbeperking door toepassing van de criteria voor de

[908] Samenvatting gebaseerd op paragraaf 5.5 van dit onderzoek.

bescherming van fundamentele rechten.

Verwerkingsbeperking door strikte interpretaties van de doelspecificatie

Het Europees gegevensbeschermingsrecht kent twee vormen van voorgeschreven verwerkingsbeperking op basis van strikte interpretaties van de doelspecificatie.[909] Beiden zijn te vinden in de Rgp.

Bij de eerste vorm is de strikte doelspecificatie opgenomen in de wet en is deze gekoppeld aan de uitoefening van de rechten van de betrokkenen. Wanneer het de verwerkingsverantwoordelijke niet helemaal duidelijk is of het verzoek tot bijvoorbeeld het wissen van de gegevens afkomstig is van de betrokkenen zelf, kan de verantwoordelijke de verzoeker om aanvullende persoonsgegevens vragen ter identificatie van de verzoeker om zo de rechtmatigheid van het verzoek te kunnen verifiëren alvorens hierop te beslissen. Ingevolge recital 41 Rgp mag die aanvullende informatie uitsluitend worden verwerkt voor het specifieke doel van identificatie en mag die informatie niet langer worden opgeslagen dan voor dat doel noodzakelijk is. Voor dit type informatie geldt dus geen verwerkingsbeperking op basis van verenigbaarheid van doeleinden of beperking door toepassing van de criteria voor de bescherming van fundamentele rechten.

Bij de tweede vorm van strikte verwerkingsbeperking wordt de doelspecificatie bepaald door de verwerkingsverantwoordelijke die gegevens aan een andere verantwoordelijke overhandigt. Onder de Rgp kan een bevoegde autoriteit gegevens doorzenden naar derde landen en internationale organisaties als er passende waarborgen voor de bescherming van de persoonsgegevens worden geboden. De Rgp noemt als voorbeelden vertrouwelijkheid en het beginsel dat de gegevens niet worden verwerkt voor *andere doeleinden* dan die waarvoor zij worden doorgegeven. *Andere doeleinden* is een striktere criterium dan dat uit het vereiste van niet-onverenigbaarheid voortvloeit: onverenigbare doeleinden. Doelen kunnen immers anders zijn maar nog steeds verenigbaar.

[909] Samenvatting gebaseerd op paragraaf 5.7 van dit onderzoek.

Conclusie en aanbevelingen

Door het apart bespreken van de twee componenten van het doelbindingsbeginsel geeft dit onderzoek een frisse kijk op de rol van het doelbindingsbeginsel in het gegevensbeschermingsrecht en in de bescherming van fundamentele rechten. De hoofdconclusie van dit onderzoek is dat de beschermende waarde van het doelbindingsbeginsel voornamelijk voortvloeit uit de rol die het doelspecificatievereiste speelt in het gegevensbeschermingsrecht en voor de bescherming van fundamentele rechten.

Twee verschillende functies van het doelspecificatievereiste zijn onderscheiden: de autonome functie die de regel neerlegt dat gegevens enkel voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden mogen worden verzameld, en de conditionele functie, waarbij het vereiste direct of indirect van invloed is op de toepasbaarheid, toepassing en uitkomst van andere regels binnen het gegevensbeschermingsrecht. Deze laatste functie weeft het doelbindingsbeginsel door het hele gegevensbeschermingsraamwerk. Directe afhankelijkheid van de doelspecificatievereiste betekent dat nadere regels afhankelijk zijn van de status die het vereiste heeft binnen het gegevensbeschermingsrecht als poot van een prominent gegevensbeschermingsbeginsel: het doelbindingsbeginsel. Indirecte afhankelijkheid slaat op de afhankelijkheid van andere regels uit het gegevensbeschermingsrecht op de verwerkingsdoeleinden of op de doelspecificatie.

De resultaten van dit onderzoek duiden op een hiërarchie in de gegevensbeschermingsbeginselen.[910] Alle gegevensbeschermingsbeginselen moeten in acht worden genomen om de rechtmatigheid van de verwerking te waarborgen. Echter voor het vereiste van niet-onverenigbaarheid van het doelbindingsbeginsel zijn rechtmatig een aantal afwijkingen toegestaan. Deze afwijkingen hoeven niet alleen als uitzondering te worden toegepast. Dit is iets dat voor een beperking wel geldt. Het minimale gegevensverwerking-, opslagbeperking- transparantie-, en juistheidbeginsel kunnen in uitzonderlijke gevallen rechtmatig worden beperkt. Voor het doelspecificatievereiste van het doelbindingsbeginsel, het rechtmatigheids- en behoorlijkheidsbeginsel, en het integriteits- en vertrouwelijkheidsbeginsel zijn zowel geen beperkingen als afwijkingen toegestaan omdat deze beginselen in het tweede lid van art. 8 Hv zijn vastgelegd of omdat het HvJEU de beginselen in verband heeft gebracht met de

[910] Samenvatting gebaseerd op paragraaf 5.2.1 van dit onderzoek.

kern van het fundamenteel recht op bescherming van persoonsgegevens. Het vereiste van niet-onverenigbaarheid wordt in de jurisprudentie geen enkele keer in verband gebracht met het fundamenteel recht op bescherming van persoonsgegevens.

Het doelbindingsbeginsel heeft twee vereisten met alle twee een geheel andere status: het vereiste van niet-onverenigbaarheid kent wettelijke afwijkingen terwijl het doelspecificatievereiste tot de kern van het fundamenteel recht op bescherming van persoonsgegevens behoort.

De afwijking die onder de Rgp is toegestaan legt geen additionele verwerkingsbeperking op de verantwoordelijke. In beginsel zou voor gegevensverwerking onder de Rgp de beperking moeten worden ingevuld door de verenigbaarheid van doeleinden, echter de toegestane afwijking hierop bestaat uit het vervullen van criteria waar de verantwoordelijke reeds aan moet voldoen: de criteria voor de bescherming van fundamentele rechten. Hierdoor verschuift de standaard verwerkingsbeperking binnen de strafvordering van verwerkingsbeperking op basis van verenigbaarheid van doeleinden naar verwerkingsbeperking door toepassing van de criteria ter bescherming van fundamentele rechten.

Uit de jurisprudentie analyse blijkt dat het doelspecificatievereiste is verbonden aan alle criteria ter bescherming van fundamentele rechten: het legitieme doel, voorzien bij wet en noodzakelijkheid in een democratische samenleving. Door de autonome en conditionele functie van het doelspecificatiebeginsel betekent verandering aan het doelbindingsbeginsel een verandering in de bescherming die het gegevensbeschermingsrecht biedt en de bescherming van fundamentele rechten.

De bepalende factoren van de verenigbaarheidstoets uit de Avg komen ook allen terug in de jurisprudentie van het EHRM. Het EHRM hanteert absoluut geen gestructureerde verenigbaarheidstoets maar de overwegingen die aan de factoren raken kunnen worden gebruikt om de factoren in te kleuren. Daarnaast heeft het EHRM in zaken waarbij gegevens verder werden gebruikt in een context die onder de Avg zou vallen, vergelijkbare factoren gebruikt om het hergebruik te toetsen. Naast verwerkingsbeperking op basis van verenigbaarheid van doeleinden en verwerkingsbeperking aan de hand van de criteria voor de bescherming van fundamentele rechten, kent het Europees gegevensbeschermingsrecht ook verwerkingsbeperking op basis van geprivilegieerde doeleinden, en verwerkingsbeperking op basis van strikte interpretaties van de doelspecificatie.

Vrijwillige doorzending van gegevens voor de detectie van strafbare feiten aan bevoegde autoriteiten worden door Recital 50 Avg beheerst, welke een smal toepassingsbereik heeft. Recital 50 verwijst naar de verwerkingsgrond, de f-grond. Voor deze verwerkingsgrond is geen afwijking opgenomen voor het vereiste van niet-onverenigbaarheid. Dat betekent dat de gegevens al moeten zijn verzameld voor het doel van doorzending voor de detectie van strafbare feiten. Dit doeleinde moet ook kenbaar zijn gemaakt bij de betrokken partijen. Recital 50 Avg voorziet in de *ad hoc* doorzending van gegevens die aan een strafbaar feit relateren. De bepaling kan niet worden gebruikt voor het delen van bulk gegevens. Voor het delen van gegevens die zijn geselecteerd omdat zij aan een profiel voldoen, geeft de wetgever geen duidelijkheid.

Bij het vaststellen van aansprakelijkheid voor de inmenging of schending van fundamentele rechten in samenwerkingsverbanden tussen private partijen en bevoegde autoriteiten hanteert het EHRM een ander criterium dan de Avg en Rgp hanteren voor verantwoordelijke en verwerker. Het EHRM kijkt naar de duur van de samenwerking, de inbreng van de overheid, het belang van de opsporingsautoriteiten bij de inmenging en de controle die de autoriteiten uitoefenden over de beslissingen en handelingen van de private partij. Dit kan betekenen dat, ondanks dat de private partij verwerkingsverantwoordelijke is onder de Avg omdat de private partij de doeleinden en de middelen bepaalt, de bevoegde autoriteit onder het EVRM verantwoordelijk kan worden gehouden voor de eventuele schendingen door de gegevensverwerking. Zodra de gegevens zijn doorgezonden heeft de private partij geen controle meer op de doeleinden van de verwerking omdat die niet meer door de verenigbaarheid van doeleinden wordt bepekt maar door de criteria voor de bescherming van fundamentele rechten en er hierdoor geen link meer is met het initiële doel en de doelen van verdere verwerking. Indien de gegevens onrechtmatig zijn verkregen door de private partij, heeft de rechtmatigheid van de verwerking door de bevoegde autoriteiten na een verplichte doorzending hier niet onder te lijden. De wet regelt niet over het effect van onrechtmatig verkregen gegevens als die vrijwillig zijn doorgezonden door de private partij.

Op basis van deze conclusie is de aanbeveling aan de Europese wetgever als volgt: verduidelijk het raamwerk rondom vrijwillige gegevensuitwisselingen voor de detectie van strafbare feiten zodat de fundamentele rechten adequaat worden gewaarborgd. Aan het maatschappelijk middenveld wordt aangeraden om op basis van de

conclusies uit deze studie strategische procedures te starten tegen het gebruik van *predictive policing* systemen in Europa waarvoor commerciële bulk data wordt verzameld.

Bibliography

[WEF, 2011] (2011). *Personal Data: The Emergence of a New Asset Class*. World Economic Forum.

[Ammon, 2006] Ammon, U. (2006). Language conflicts in the European Union. *International Journal of Applied Linguistics*, 16(3):319–338.

[Amos, 2017] Amos, M. (2017). The Value of the European Court of Human Rights to the United Kingdom. *European Journal of International Law*, 28(3):763–785.

[Angelis and Harrison, 2003] Angelis, T. J. and Harrison, J. H. (2003). History and importance of the rule of law. Technical report, World Justice Project.

[Ballaschk, 2015] Ballaschk, J. (2015). In the Unseen Realm: Transnational Intelligence Sharing in the European Union-Challenges to Fundamental Rights and Democratic Legitimacy. *Stan. J. Int'l L.*, 51:19.

[Bennett, 1992] Bennett, C. J. (1992). *Regulating privacy: Data protection and public policy in Europe and the United States*. Cornell University Press.

[Bigo et al., 2012] Bigo, D., Carrera, S., Hayes, B., Hernanz, N., and Jeandesboz, J. (2012). Justice and Home Affairs Databases and a Smart Borders System at EU External Borders: An Evaluation of Current and Forthcoming Proposals. *CEPS Papers in Liberty and Security in Europe*, (52).

[Bingham, 2007] Bingham, L. (2007). The rule of law. *The Cambridge Law Journal*, 66(01):67–85.

[Blaustein, 1964] Blaustein, E. (1964). Privacy as an aspect of human dignity. *New York Law Review*, 39:962–1007.

[Bobek, 2008] Bobek, M. (2008). Learning to talk: preliminary rulings, the courts of the new member states and the Court of Justice. *Common Market L. Rev.*, 45:1611.

[Borgesius, 2014] Borgesius, F. J. Z. (2014). Improving privacy protection in the area of behavioural targeting. *Available at SSRN 2654213*.

[Borgesius, 2016] Borgesius, F. J. Z. (2016). Singling out people without knowing their names–behavioural targeting, pseudonymous data, and the new data protection regulation. *Computer Law & Security Review*, 32(2):256–271.

[Borgesius, 2018] Borgesius, F. J. Z. (2018). *Discrimination, artificial intelligence, and algorithmic decision-making*. Council of Europe.

[Brkan, 2017] Brkan, M. (2017). In search of the concept of essence of EU fundamental rights through the prism of data privacy. *Maastricht Faculty of Law Working Paper*, (2017-01).

[Brkan, 2019] Brkan, M. (2019). The essence of the fundamental rights to privacy and data protection: Finding the way through the maze of the cjeuÕs constitutional reasoning. *German Law Journal*, 20(6):864Ð883.

[Brouwer, 2008] Brouwer, E. (2008). *Digital borders and real rights: effective remedies for third-country nationals in the Schengen Information System*. Nijhoff, Leiden, the Netherlands.

[Brouwer, 2011] Brouwer, E. (2011). Legality and data protection law: The forgotten purpose of purpose limitation. *European monographs*, 75:273–294.

[Buttarelli, 2016] Buttarelli, G. (2016). The EU GDPR as a clarion call for a new global digital gold standard. *International Data Privacy Law*, 6(2):77–78.

[Bygrave, 1998] Bygrave, L. A. (1998). Data protection pursuant to the right to privacy in human rights treaties. *International Journal of Law and Information Technology*, 6(3):247–284.

[Bygrave, 2017] Bygrave, L. A. (2017). Data Protection by Design and by Default: Deciphering the EU's Legislative Requirements. *Oslo Law Review*, 4(02):105–120.

[Cannataci et al., 2006a] Cannataci, Caruana, and Bonnici (2006a). *Monitoring, Supervision and Information Technology*, chapter R(87) 15: A slow death?, pages 27 – 49. In [Cannataci et al., 2006b].

[Cannataci et al., 2006b] Cannataci, Caruana, and Bonnici (2006b). *Monitoring, Supervision and Information Technology*. Erasmus University Press, Rotterdam.

[Cannataci and Bonnici, 2010] Cannataci, J. A. and Bonnici, J. P. M. (2010). The end of the purpose-specification principle in data protection? *Int. Rev. Law Comput. Technol.*, 24(1):101–117.

[Cate, 2016] Cate, F. H. (2016). *The failure of fair information practice principles*. Routledge.

[Cavoukian et al., 2009] Cavoukian, A. et al. (2009). Privacy by design: The 7 foundational principles. implementation and mapping of fair information practices. *Information and Privacy Commissioner of Ontario, Canada*, 5.

[Chesterman, 2008] Chesterman, S. (2008). An international rule of law? *American Journal of Comparative Law*, 56(2):331–362.

[Clarke, 1991] Clarke, R. (1991). The tax file number scheme: A case study of political assurances and function creep. *Policy*, 7(4).

[Cleiren et al., 1990] Cleiren, C. et al. (1990). Identiteit van beginselen van behoorlijke strafrechtspleging en beginselen van behoorlijk bestuur?

[Colonna, 2014] Colonna, L. (2014). Data mining and its paradoxical relationship to the purpose limitation principle. In *Reloading Data Protection*, pages 299–321. Springer.

[Coudert, 2017] Coudert, F. (2017). The Europol Regulation and Purpose Limitation: From the Silo Based Approach to What Exactly. *Eur. Data Prot. L. Rev.*, 3:313.

[Coudert et al., 2012] Coudert, F., Dumortier, J., and Verbruggen, F. (2012). Applying the purpose specification principle in the age of big data: the example of integrated video surveillance platforms in France. *ICRI Working papers*, 6.

[Coudert and Werkers, 2008] Coudert, F. and Werkers, E. (2008). In the aftermath of the promusicae case: how to strike the balance? *International Journal of Law and Information Technology*, 18(1):50–71.

[Craig, 1997] Craig, P. (1997). Formal and substantive conceptions of the rule of law: an analytical framework. *Public Law*, pages 467–487.

[Craig, 2007] Craig, P. (2006-2007). The rule of law, hl 151. Technical report, Parliament papers, Apendix 5.

[Crawford, 2015] Crawford, M. (2015). Introduction: Attention as a cultural problem. *The world beyond your head: on becoming an individual in an age of distraction*, pages 3–30.

[Curry et al., 2004] Curry, M. R., Phillips, D. J., and Regan, P. M. (2004). Emergency response systems and the creeping legibility of people and places. *The Information Society*, 20(5):357–369.

[De Busser, 2009a] De Busser, E. (2009a). *Data protection in EU and US criminal cooperation: A substantive law approach to the EU internal and transatlantic cooperation in criminal matters between judicial and law enforcement authorities*. Maklu.

[De Busser, 2009b] De Busser, E. (2009b). Purpose limitation in eu-us data exchange in criminal matters: the remains of the day. In Cools, M., De Kimpe, S., De Ruyver, B., Easton, M., Pauwels, L., Ponsaers, P., Vande Walle, G., Vander Beken, T., Vander Laenen, F., and Vermeulen, G., editors, *Readings on criminal justice, criminal law and policing*, volume 2 of *Governance of Security Research Paper Series*, pages 163–201. Maklu.

[De Hert and Gutwirth, 2006a] De Hert, P. and Gutwirth, S. (2006a). Interoperability of police databases within the eu: an accountable political choice? *International Review of Law Computers & Technology*, 20(1-2):21–35.

[De Hert and Gutwirth, 2006b] De Hert, P. and Gutwirth, S. (2006b). Privacy, data protection and law enforcement. opacity of the individual and transparency of power. *Privacy and the criminal law*, pages 61–104.

[De Montesquieu, 1989] De Montesquieu, C. (1989). *Montesquieu: The Spirit of the Laws*. Cambridge University Press.

[de Secondat et al., 2001] de Secondat, C., Carrithers, D. W., Mosher, M. A., and Rahe, P. A. (2001). *Montesquieu's Science of Politics: Essays on the Spirit of Laws*. Rowman & Littlefield.

[Douglas-Scott, 2014] Douglas-Scott, S. (2014). A tale of two courts: Luxembourg, Strasbourg and the growing European human rights acquis. *Strasbourg and the Growing European Human Rights Acquis (June 24, 2014)*, 43.

[Evers, 2016] Evers, J. (2016). Disclosing medical data: A foreseeable application of the law. *Eur. Data Prot. L. Rev.*, 2:432.

[Fazlioglu, 2013] Fazlioglu, M. (2013). Forget me not: the clash of the right to be forgotten and freedom of expression on the internet. *International Data Privacy Law*, 3(3):149–157.

[Foqué and Hart, 1990] Foqué, R. M. and Hart, A. C. (1990). *Instrumentaliteit en rechtsbescherming: grondslagen van een strafrechtelijke waardendiscussie*. Gouda Quint.

[Forgó et al., 2017] Forgó, N., Hänold, S., and Schütze, B. (2017). The principle of purpose limitation and big data. In *New Technology, Big Data and the Law*, pages 17–42. Springer.

[Friedman, 1990] Friedman, L. M. (1990). *The republic of choice: Law, authority, and culture*. Harvard University Press.

[Fuster, 2014a] Fuster, G. G. (2014a). Fighting for your right to what exactly-the convoluted case law of the eu court of justice on privacy and/or personal data protection. *Birkbeck L. Rev.*, 2:263–278.

[Fuster, 2014b] Fuster, G. G. (2014b). *The emergence of personal data protection as a fundamental right of the European Union*. Law, Governance and Technology Series. Springer, Berlin.

[Fuster and Gutwirth, 2013] Fuster, G. G. and Gutwirth, S. (2013). Opening up personal data protection: A conceptual controversy. *Computer Law & Security Review*, 29(5):531–539.

[Gellman, 2002] Gellman, R. (2002). Privacy, finding a balanced approach to consumer options. *Center for democracy and technology*, pages 1–7.

[Gellman, 2017] Gellman, R. (2017). Fair information practices: A basic history. *Available at SSRN 2415020*.

[Gerards and Senden, 2009] Gerards, J. and Senden, H. (2009). The structure of fundamental rights and the european court of human rights. *International journal of constitutional law*, 7(4):619–653.

[Ghani et al., 2016] Ghani, N. A., Hamid, S., and Udzir, N. I. (2016). Big data and data protection: Issues with purpose limitation principle. *International Journal of Advances in Soft Computing & Its Applications*, 8(3).

[Guild and Carrera, 2014] Guild, E. and Carrera, S. (2014). The political and judicial life of metadata: Digital rights ireland and the trail of the data retention directive. *CEPS Liberty and Security in Europe Papers*, (65).

[Gutwirth, 1993] Gutwirth, S. (1993). De toepassing van het finaliteitsbeginsel van de privacywet van 8 december 1992 tot bescherming van de persoonlijke levenssfeer ten opzichte van de verwerking van persoonsgegevens?[the application of the purpose specification principle in the belgian data protection act of 8 december 1992]. *Tijdschrift voor Privaatrecht-TPR*, 1993(4):1409–1477.

[Gutwirth and de Hert, 2009] Gutwirth, S. and de Hert, P. (2009). *Reinventing data protection?*, chapter Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action. In [Gutwirth et al., 2009].

[Gutwirth et al., 2009] Gutwirth, S., Poullet, Y., de Hert, P., de Terwangne, C., and Nouwt, S. (2009). *Reinventing data protection?* Springer.

[Hildebrandt, 2008] Hildebrandt, M. (2008). Profiling and the identity of the european citizen. In *Profiling the European Citizen*, pages 303–343. Springer.

[Hildebrandt, 2013] Hildebrandt, M. (2013). Slaves to big data. or are we? *IDP. Revista de Internet, Derecho y Ciencia Política*, (17).

[Hildebrandt, 2014] Hildebrandt, M. (2014). Location data, purpose binding and contextual integrity: What's the message? In *Protection of Information and the Right to Privacy-A New Equilibrium?*, pages 31–62. Springer.

[Hildebrandt, 2015a] Hildebrandt, M. (2015a). Radbruch's rechtsstaat and schmitt's legal order: Legalism, legality, and the institution of law. *Critical Analysis of Law*, 2(1).

[Hildebrandt, 2015b] Hildebrandt, M. (2015b). *Smart technologies and the end (s) of law: novel entanglements of law and technology*. Edward Elgar Publishing.

[Hix and Høyland, 2011] Hix, S. and Høyland, B. (2011). *The political system of the European Union*. Palgrave Macmillan.

[Hutchinson, 1999] Hutchinson, M. R. (1999). The margin of appreciation doctrine in the european court of human rights. *International & Comparative Law Quarterly*, 48(3):638–650.

[James R. Silkenat, 2014] James R. Silkenat, James E. Hickey Jr., P. D. B., editor (2014). *The legal doctrines of the rule of law and the legal state (Rechtsstaat)*. Springer, Berlin.

[Jansen, 2019] Jansen, F. (2019). Data-driven policing in the context of europe. Technical report, Working Paper, Data Justice Project.

[Jasserand, 2018] Jasserand, C. (2018). Subsequent use of GDPR data for a law enforcement purpose: The forgotten principle purpose limitation. *Eur. Data Prot. L. Rev.*, 4:152.

[Kokott and Sobotta, 2013] Kokott, J. and Sobotta, C. (2013). The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR. *International Data Privacy Law*, 3(4):222–228.

[Koning et al., 2014] Koning, M., Korenhof, P., Alpár, G., and Hoepman, J.-H. (2014). The ABCs of ABCs: an analysis if attribute-based credentials in the light of data protection, privacy and identity. *Online proceeding HotPets*.

[Koops, 2011] Koops, B.-J. (2011). The (in) flexibility of techno-regulation and the case of purpose-binding. *Legisprudence*, 5(2):171–194.

[Koot, 2012] Koot, M. R. (2012). *Measuring and Predicting Anonymity*. PhD thesis, University of Amsterdam, Amsterdam, The Netherlands.

[Kosta, 2013a] Kosta, E. (2013a). *Consent in European Data Protection Law*. Brill, Leiden.

[Kosta, 2013b] Kosta, E. (2013b). The way to Luxemburg: national court decisions on the compatibility of the data retention directive with the rights to privacy and data protection. *SCRIPTed*, 10:339.

[Krisch, 2008] Krisch, N. (2008). The open architecture of European human rights law. *Modern Law Review*, 71(2):183.

[Kuner, 2008] Kuner, C. B. (2008). Data protection and rights protection on the internet: The Promusicae judgment of the European Court of Justice. *European Intellectual Property Review*, 30(5):199–202.

[Kunig, 1986] Kunig, P. (1986). *Das Rechtsstaatsprinzip: Überlegungen zu seiner Bedeutung für das Verfassungsrecht der Bundesrepublik Deutschland*. Mohr Siebeck.

[Lenaerts, 2012] Lenaerts, K. (2012). Exploring the limits of the EU Charter of Fundamental Rights. *European Constitutional Law Review*, 8:375–403.

[Letki, 2002] Letki, N. (2002). Lustration and democratisation in East-Central Europe. *Europe-Asia Studies*, 54(4):529–552.

[Letourneur and Drago, 1958] Letourneur, M. and Drago, R. (1958). The Rule of Law as Understood in France. *The American Journal of Comparative Law*, pages 147–177.

[Letsas, 2004] Letsas, G. (2004). The truth in autonomous concepts: How to interpret the ECHR. *European Journal of International Law*, 15(2):279–305.

[Licht et al., 2007] Licht, A. N., Goldschmidt, C., and Schwartz, S. H. (2007). Culture rules: The foundations of the Rule of Law and other norms of governance. *Journal of comparative economics*, 35(4):659–688.

[Loughlin, 2010] Loughlin, M. (2010). *Foundations of public law*. Oxford University Press.

[Lynskey, 2015] Lynskey, O. (2015). *The foundations of EU data protection law*. Oxford University Press.

[Lyon and Bauman, 2013] Lyon, D. and Bauman, Z. (2013). *Liquid surveillance: A conversation*. John Wiley & Sons.

[Marcinkowski, 2013] Marcinkowski, B. M. (2013). Privacy paradox (es): In search of a transatlantic data protection standard. *Ohio St. LJ*, 74:1167.

[Mathias Kötter, 2014] Mathias Kötter, G. F. S. (2014). *The legal doctrines of the rule of law and the legal state (Rechtsstaat)*, chapter Applying the Rule of Law to Contexts Beyond the State. In [James R. Silkenat, 2014].

[Mayer-Schonberger and Padova, 2015] Mayer-Schonberger, V. and Padova, Y. (2015). Regime Change: Enabling Big Data through Europe's New Data Protection Regulation. *Colum. Sci. & Tech. L. Rev.*, 17:315.

[Moerel et al., 2016] Moerel, Prins, Hildebrandt, Tai, T. T., Zwenne, and Schmidt (2016). 146e jaargang, 2016, "homo digitalis", preadviezen. *Vereniging, Handelingen Nederlandse Juristen*.

[Moerel and Prins, 2016] Moerel, L. and Prins, C. (2016). Privacy for the homo digitalis: Proposal for a new regulatory framework for data protection in the light of big data and the internet of things. *Available at SSRN 2784123*.

[Moravcsik, 2000] Moravcsik, A. (2000). The origins of human rights regimes: Democratic delegation in postwar europe. *International Organization*, 54(2):217–252.

[Mowbray, 2004] Mowbray, A. (2004). *The development of positive obligations under the European Convention on Human Rights by the European Court of Human Rights*. Bloomsbury Publishing.

[Nissenbaum, 2015] Nissenbaum, H. (2015). *Respect for context as a benchmark for privacy online: what it is and isn't*, pages 278–302. Cambridge University Press.

[O'Donnell, 2004] O'Donnell, G. A. (2004). Why the rule of law matters. *Journal of Democracy*, 15(4):32–46.

[O'Donnell, 1982] O'Donnell, T. A. (1982). The margin of appreciation doctrine: standards in the jurisprudence of the European Court of Human Rights. *Hum. Rts. Q.*, 4:474.

[Ojanen, 2016] Ojanen, T. (2016). Making the essence of fundamental rights real: the court of justice of the European Union clarifies the structure of fundamental rights under the Charter. *European Constitutional Law Review*, 12(2):318–329.

[Oostveen and Irion, 2018] Oostveen, M. and Irion, K. (2018). The golden age of personal data: How to regulate an enabling fundamental right? In *Personal Data in Competition, Consumer Protection and Intellectual Property Law*, pages 7–26. Springer.

[Paine, 2004] Paine, T. (2004). *Common sense*. Broadview Press.

[Pech, 2009] Pech, L. (2009). *The Rule of Law as a constitutional principle of the European Union*. Jean Monnet Working Paper Series.

[Poullet and Rouvroy, 2009] Poullet, Y. and Rouvroy, A. (2009). *Reinventing data protection?*, chapter The right to informational self-determination and the value of self-development: Reassessing the importance of privacy for democracy. In [Gutwirth et al., 2009].

[Purtova, 2018] Purtova, N. (2018). Between the GDPR and the Police Directive: navigating through the maze of information sharing in public–private partnerships. *International Data Privacy Law*, 8(1):52–68.

[Raab, 2016] Raab, C. D. (2016). Information privacy: Ethics and accountability. *Available at SSRN 3057469*.

[Radin, 1989] Radin, M. J. (1989). Reconsidering the rule of law. *BUL Rev.*, 69:781.

[Rahe et al., 2001] Rahe, P. A., Carrithers, D. W., and Mosher, M. A. (2001). *Montesquieu's Science of Politics: Essays on the Spirit of Laws*. Rowman & Littlefield Publishers.

[Rauhofer, 2015] Rauhofer, J. (2015). Of Men and Mice: Should the EU Data Protection Authorities' Reaction to Google's New Privacy Policy Raise Concern for the Future of the Purpose Limitation Principle. *Eur. Data Prot. L. Rev.*, 1:11.

[Raz, 1977] Raz, J. (1977). The rule of law and its virtue. In *The Rule of Law and the Separation of Powers*, pages 77–94. Routledge.

[Risse and Ropp, 1999] Risse, T. and Ropp, S. C. (1999). *International human rights norms and domestic change: conclusions*, pages 234–278. Cambridge University Press, Cambridge.

[Rodotà, 2009] Rodotà, S. (2009). *Data protection as a fundamental right*, pages 77–82. In [Gutwirth et al., 2009].

[Roessler, 2015] Roessler, Beate, M. D., editor (2015). *Social dimension of Privacy*. Cambridhge University Press, Cambridge.

[Rosen, 2000] Rosen, J. (2000). The unwanted gaze. *The Destruction of Privacy in America (New York: Vintage, 2001)*.

[Rosenfeld, 2001] Rosenfeld, M. (2001). The rule of law and the legitimacy of constitutional democracy. *Cardozo Law School, Public Law Research Paper*, (36).

[Ryssdal, 1991] Ryssdal, R. (1991). Data Protection and the European Convention on Human Rights in Council of Europe. Data protection, human rights and democratic values. In *XIII Conference of the Data Commissioners*, pages 2–4.

[Salami, 2017] Salami, E. (2017). The impact of directive (EU) 2016/680 on the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties and on the free movement of such data on the existing privacy regime. *Investigation, Detection or Prosecution of Criminal Offences or the Execution of Criminal Penalties and on the Free Movement of Such Data on the Existing Privacy Regime (February 6, 2017)*.

[Scalia, 1989] Scalia, A. (1989). The rule of law as a law of rules. *The University of Chicago Law Review*, pages 1175–1188.

[Schermer, 2011] Schermer, B. W. (2011). The limits of privacy in automated profiling and data mining. *Computer Law & Security Review*, 27(1):45–52.

[Sharandin and Kravchenko, 2014] Sharandin, Y. A. and Kravchenko, D. V. (2014). *The legal doctrines of the rule of law and the legal state (Rechtsstaat)*, chapter Rule of Law, Legal State and Other International Legal Doctrines: Linguistic Aspects of Their Convergence and Differentioation. In [James R. Silkenat, 2014].

[Snell, 2015] Snell, J. (2015). Fundamental rights review of national measures: Nothing new under the charter? *European Public Law*, 21(2):285–308.

[Stalla-Bourdillon and Knight, 2018] Stalla-Bourdillon, S. and Knight, A. (2018). Data analytics and the GDPR: friends or foes? A call for a dynamic approach to data protection law.

[Sweeney, 2002] Sweeney, L. (2002). k-anonymity: A model for protecting privacy. *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, 10(05):557–570.

[Tamanaha, 2012] Tamanaha, B. (2012). The history and elements of the rule of law. *Singapore Journal of Legal Studies*, page 232.

[Tene, 2013] Tene, O. (2013). Privacy law's midlife crisis: A critical assessment of the second wave of global privacy laws. *Ohio St. LJ*, 74:1217.

[Tiedeman, 2014] Tiedeman, P. (2014). *The legal doctrines of the rule of law and the legal state (Rechtsstaat)*, chapter The Rechtsstaat-Principle in Germany: The Development from the Beginning Until Now. In [James R. Silkenat, 2014].

[Tzanou, 2017] Tzanou, M. (2017). *The fundamental right to data protection: normative value in the context of counter-terrorism surveillance*. Bloomsbury Publishing.

[van der Sloot, 2015] van der Sloot, B. (2015). Annotatie bij Hof van Justitie van de EU 11 december 2014 (Ryneš). *European Human Rights Cases*, 3(47).

[Voigt and von dem Bussche, 2017] Voigt, P. and von dem Bussche, A. (2017). Enforcement and fines under the gdpr. In *The EU General Data Protection Regulation (GDPR)*, pages 201–217. Springer.

[von Grafenstein, 2018] von Grafenstein, M. (2018). *The Principle of Purpose Limitation in Data Protection Laws*. Nomos, Hamburg.

[Westin, 1967] Westin, A. F. (1967). *Privacy and freedom*. Atheneum Press, New York.

[Westin, 2003] Westin, A. F. (2003). Social and political dimensions of privacy. *Journal of social issues*, 59(2):431–453.

[Wiebe and Dietrich, 2017] Wiebe, A. and Dietrich, N. (2017). *Open Data Protection-Study on legal barriers to open data sharing-Data Protection and PSI*. Universitätsverlag Göttingen.

[WODC, 2011] WODC (2011). *Juridische verkenningen 2011, nr. 8: Function creep en privacy*. Boom Juridische uitgevers.

[Wolters, 2017] Wolters, P. (2017). The security of personal data under the GDPR: a harmonized duty or a shared responsibility? *International Data Privacy Law*, 7(3):165–178.

[Wright et al., 2011] Wright, D., De Hert, P., and Gutwirth, S. (2011). Are the OECD guidelines at 30 showing their age? *Communications of the ACM*, 54(2):119–127.

[Zarsky, 2013] Zarsky, T. Z. (2013). Transparent predictions. *U. Ill. L. Rev.*, page 1503.

[Zarsky, 2015] Zarsky, T. Z. (2015). The privacy-innovation conundrum. *Lewis & Clark L. Rev.*, 19:115.

[Zarsky, 2016] Zarsky, T. Z. (2016). Incompatible: The GDPR in the Age of Big Data. *Seton Hall L. Rev.*, 47:995.

[Zuboff, 2019] Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. Profile Books.

Case law

European Court of Human Rights

EComHR 12 October 1973, no. 5877/72 (*X/the United Kingdom*).
EComHR 18 May 1976, no. 6825/74 (*X/Iceland*).
ECtHR 8 June 1976, no. 5100/71, 5101/71, 5102/71, 5354/72, 5370/72, (*Engel And Others/he Netherlands*).
ECtHR 7 December 1976, no. 5095/71, 5920/72, 5926/72, (*Kjeldsen, Busk Madsen and Pedersen/Denmark*).
ECtHR 25 April 1978, no. 5856/72, (*Tyrer/the United Kingdom*).
ECtHR 6 September 1978, no. 5029/71 (*Klass and others/Federal Republic of Germany*).
ECtHR 26 April 1979 , no.6538/74 (*Sunday Times/the United Kingdom*).
ECtHR 23 September 1981, no. 7525/76, (*Dudgeon/United Kingdom*).
ECtHR 25 March 1983, no. 5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75, 7136/75) (*Silver and Others/the United Kingdom*)
ECtHR 2 Augustus 1984, no. 8691/79 (*Malone/the United Kingdom*).
ECtHR 26 March 1987, no. 9248/81, (*Leander/Sweden*).
ECtHR 7 July 1989, no. 14038/88, (*Soering/the United Kingdom*).
ECtHR 7 July 1989, no.10454/83 (*Gaskin/the United Kingdom*).
ECtHR 22 February 1989, no. 11508/85 (*Barfod/Denmark*).

EComHR 9 February 1990, no. 13258/87 (*M. and Co./the Federal Republic of Germany*).
ECtHR 24 April 1990, 4, no.11105/84 (*Huvig/France*).
ECtHR 24 April 1990, no. 11801/85 (*Kruslin/France*).
ECtHR 30 August 1990, no. 12244/86, 12245/86, 12383/86 (*Fox, Campbell and Hartley/the United Kingdom*).
ECtHR 25 March 1992, no. 13590/88 (*Campbell/the United Kingdom*).
EComHR 7 December 1992, no. 18395/91 (*Lupker/the Netherlands*).
ECtHR 16 December 1992, no. 13710/88 (*Niemietz/Federal Republic of Germany*).
ECtHR 23 November 1993, no. 14838/89 (*A./France*).
ECtHR 28 October 1994, no. 14310/88 (*Murray/the United Kingdom*).
EComHR 31 January 1995, no. 18395/91 (*Friedl/Austria*).
EComHR 18 May 1995, no. 22942/93 (*R. L. v The Netherlands*).
ECtHR 25 February 1997, no. 22009/93 (*Z/Finland*).
ECtHR 25 June 1997, no. 20605/92 (*Halford/the United Kingdom*).
ECtHR 27 Augustus 1997, no. 20837/92 (*M.S./Sweden*).
EComHR 14 January 1998, no. 32200/96 (*Herbecq and the Association 'Ligue des Droits de l'homme'/Belgium*).
ECtHR 25 March 1998, no. 23224/94 (*Kopp/Switzerland*).
ECtHR 24 August 1998, no. 23618/94 (*Lambert/France*).
ECtHR 26 January 1999, no. 42293/98 (*Adamson/the United Kingdom*).
ECtHR 20 May 1999, no. 25390/94, (*Rekv̀enyi/Hungary*).
ECtHR 14 September 1999, no. 32441/96 (*Karakurt/Austria*).
ECtHR 16 February 2000, no. 27798/95 (*Amann/Switzerland*).
ECtHR 4 May 2000, no. 28341/95 (*Rotaru/Romania*).
ECtHR 4 May 2000, no. 30194/09 (*Shimovolos/Russia*).
ECtHR 4 October 2000, no. 35394/97 (*Khan/the United Kingdom*).
ECtHR 25 September 2001, no.44787/98 (*P.G. and J.H./the United Kingdom*).
ECtHR 12 December 2001, no. 52207/99 (*Vlastimir and Borka Banković, Živana Stojanović, Mirjana Stoimenovski, Dragana Joksimović and Dragan Suković/Belgium, the Czech Republic, Denmark, France, Germany, Greece, Hungary, Iceland, Italy, Luxembourg, the Netherlands, Norway, Poland, Portugal, Spain, Turkey and the United Kingdom*).
ECtHR 11 July 2002, no. 28957/95, (*Christine Goodwin/the United Kingdom*).

ECtHR 28 January 2003, no. 44647/98 (*Peck/the United Kingdom*).
ECtHR 8 April 2003, no. 39339/98 (*M.M./the Netherlands*).
ECtHR 7 July 2003, no. 63737/00 (*Perry/the United Kingdom*).
ECtHR 24 June 2004, no. 59320/00 (*Von Hannover/Germany*).
ECtHR 8 July 2004, no. 48787/99 (*Ilaşcu/Moldova and Russia*).
ECtHR 16 November 2004, no. 29865/96 (*Ünal Tekeli/Turkey*).
ECtHR 11 January 2005, no. 50774/99 (*Sciacca/Italy*).
ECtHR 30 June 2005, no. 45036/98 (*Bosphorus Hava Yolları Turizm Ve Ticaret Anonim Şirketi/Ireland*).
ECtHR 6 June 2006, no. 62332/00 (*Segerstedt-Wiberg and others/Sweden*).
ECtHR 29 June 2006, no. 54934/00 (*Weber and Saravia/Germany*).
ECtHR 10 October 2006, no. 7508/02 (*L.L./France*).
EComHR 7 December 2006, no. 29514/05, (*van der Velden/the Netherlands*).
ECtHR 1 March 2007, no. 5935/02 (*Affaire Heglas/Republique Tcheque*).
ECtHR 10 March 2007, no. 4378/02 (*Bykov/Rusia*).
ECtHR 3 April 2007, no. 62617/00 (*Copland/the United Kingdom*).
ECtHR 28 June 2007, no. 62540/00 (*Association for European Integration and Human Rights and Ekimdzhiev/Bulgaria*).
ECtHR 25 October 2007, no. 38258/03 (*Vondel/the Netherlands*).
ECtHR 1 July 2008 , no.58243/00 (*Liberty and others/the United Kingdom*).
ECtHR 18 November 2008, no. 22427/04 (*Cemalettin Canli/Turkey*).
ECtHR 25 November 2008, no. 23373/03 (*Biriuk/Lithuania*).
ECtHR 2 December 2008, no. 2872/02 (*K.U./Finland*).
ECtHR 4 December 2008, no.130562/04 and 30566/04 (*S. and Marper/the United Kingdom*).
ECtHR 9 June 2009, no. 72094/01 (*Kvasnica/Slovakia*).
ECtHR 17 December 2009, no. 2115/06 (*M.B./France*).
ECtHR 17 December 2009, no. 5335/06 (*Bouchacourt/France*).
ECtHR 17 December 2009, no. 16428/05 (*Gardel/France*).
ECtHR 18 May 2010, no. 26839/05 (*Kennedy/the United Kingdom*).
ECtHR 2 September 2010, no. 35623/05 (*Uzun/Turkey*).
ECtHR 5 October 2010, no. 420/07 (*Köpke/Germany*).
ECtHR 7 July 2011, no. 27021/08 (*Al-Jedda/United Kingdom*).
ECtHR 7 July 2011, no. 55721/07 (*Case Of Al-Skeini and Others/the United King-*

dom).

ECtHR 18 October 2011, no.16188/07 (*Khelili/Switzerland*).

ECtHR 14 February 2012, no. 7094/06 (*Romet/Netherlands*).

ECtHR 30 October 2012, no. 57375/08 (*P. and S./Poland*).

ECtHR 13 November 2012, no. 24029/07 (*M.M./the United Kingdom*).

ECtHR 6 December 2012, no. 12323/11 (*Michaud/France*).

ECtHR 4 June 2013, no. 7841/08 (*Peruzzo en Martens/Germany*).

ECtHR 6 June 2013, no. 1585/09 (*Avilkina/Russia*).

ECtHR 25 June 2013, no.18540/04 (*Valentino Acatrinei/Romania*).

ECtHR 16 July 2013, no. 33846/07 (*Węgrzynowski and Smolczewski/Poland*).

ECtHR 26 November 2013, no. 27853/09 (*X/Latvia*).

ECtHR 15 April 2014, no. 50073/07 (*Radu/the Republic of Moldova*).

ECtHR 29 April 2014, no. 52019/07 (*L.H./Latvia*).

ECtHR 2 December 2014, no. 3082/06 (*Taraneks/Latvia*).

ECtHR 7 July 2015, no. 28005/12 (*M.N. and others/San Marino*).

ECtHR 4 December 2015, no. 47143/06 (*Roman Zakharov/Russia*).

ECtHR 23 February 2016, no. 40378/06 (*Y.Y./Russia*).

ECtHR 17 May 2016, nos. 33677/10 and 52340/10 (*Fürst-Pfeifer/Austria*).

ECtHR 6 June 2016, no.37138/14 (*Szabó and Vissy/Hungary*).

ECtHR 18 October 2016, no. 61838/10 (*Vukota-Bojić v. Switzerland*).

ECtHR 26 Januari 2017, no. 42788/06 (*Surikov/Ukrain*).

ECtHR 6 April 2017, no. 2229/15 (*Karajanov/the former Republic of Macedonia*).

ECtHR 27 April 2017, no. 73607/13 (*Sommer/Germany*).

ECtHR 5 September 2017, no. 61496/08 (*Bărbulescu/Romania*).

ECtHR 13 September 2018, nos. 58170/13, 62322/14 and 24960/15 (*Big Brother Watch and others/the United Kingdom*).

ECtHR 20 September 2018, no. 18925/09 (*Jishkariani/Georgia*).

Court of Justice of the European Union

CJEU 15 July 1964, C-6/64 (*Flaminio Costa/E.N.E.L.*).

CJEU 12 November 1969, C-29/69 (*Stauder*).

CJEU 17 December 1970, C-11/70, (*International Handelsgesellschaft*).

CJEU 14 May 1974, C-4/73, (*Nold*).

CJEU 13 February 1979, C-101/78, (*Granaria BV/Hoofdproduktschap voor Akkerbouwprodukten*).

CJEU 13 December 1979, C-44/79 (*Hauer*).

CJEU 7 July 1985, C-168/84, (*Gunter Berkholz/Finanzamt Hamburg-Mitte-Altstadt*).

CJEU 23 April 1986, C-294/83, (*Parti écologiste Les Verts/European Parliament*).

CJEU 15 May 1986, C-222/84, (*Johnston/Chief Constable of the Royal Ulster Constabulary*).

CJEU 13 July 1989, C-5/88 (*Wachauf*).

CJEU 21 September 1989, C-46/87 and 227/88, (*Hoechst*).

CJEU 18 June 1991, C-260/89, (*Elliniki Radiophonia Tiléorassi AE and Panellinia Omospondia Syllogon Prossopikou/Dimotiki Etairia Pliroforissis and Sotirios Kouvelas and Nicolaos Avdellas and others*).

CJEU 25 July 1991, C-221/89, (*The Queen/Secretary of State for Transport, ex parte Factortame Ltd and others*).

CJEU 15 December 1995, C-415/93 (*Bosman*).

CJEU 26 November 1996, C-68/95 (*Port*).

CJEU 29 May 1997, C-299/95, (*Kremzow*).

CJEU 7 May 1998, C-390/96, (*Lease Plan Luxembourg SA/Belgische Staat*).

CJEU 6 March 2001, C-274/99, (*Connolly/Commission*).

CJEU 22 October 2002, C-94/00, (*Roquette Frères SA*).

CJEU 20 May 2003, joined cases C-465/00, C-138/01, C-139/01, (*Rechnungshof/Österreichischer Rundfunk and Others, and Christa Neukomm and Joseph Lauermann/Österreichischer Rundfunk*).

CJEU 12 June 2003, C-112/00, (*Eugen Schmidberger, Internationale Transporte und Planzüge*).

CJEU 6 November 2003, C-101/01, (*Bodil Lindqvist*).

CJEU 25 March 2004, C-71/02 (*Karner*).

CJEU 5 October 2004, C-397/01 to C-403/0, (*Pfeiffer and others*).

Opinion A-G, CJEU 18 July 2007, C-275/06, (*Productores de Música de España (Promusicae)/Telefónica de España SAU.*).

CJEU 11 December 2007, C-438/05, (*Viking Line*).

CJEU 29 January 2008, C-275/06, (*Productores de Música de España (Promusicae)/Telefónica de España SAU*).

CJEU 14 February 2008, C-244/06 (*Dynamic Medien*).

Opinion A-G, CJEU 3 April 2008, C-275/06, (*Huber/Germany*).

Opinion A-G, CJEU 8 May 2008, C-73/07, (*Tietosuojavaltuutettu/Satakunnan Markkinapörssi Oy and Satamedia Oy*).

CJEU 3 September 2008, C-402/05 and C-415/05 (*Kadi and Al Barakaat International Foundation/Council and Commission*).

CJEU 16 December 2008, C-524/06, (*Huber/Germany*).

CJEU 16 December 2008, C-73/07, (*Tietosuojavaltuutettu/Satakunnan Markkinapörssi Oy and Satamedia Oy*).

CJEU 7 May 2009, C-553/07 (*Rijkeboer*).

CJEU 19 January 2010, C-555/07, (*Kŭcŭkdeveci*).

CJEU 9 March 2010, C-518/07 (*European Commission/Federal Republic of Germany*).

CJEU 19 November 2010, C-92/09 and C-93/09, (*Volker and Markus Schecke and Eifert*).

CJEU 23 November 2010, C-145/09 (*Tsakouridis*).

CJEU 7 December 2010, joined cases C-585/08, C-144/09, (*Peter Pammer/Reederei Karl Schlüter GmbH und Co. KG, and Hotel Alpenhof GesmbH/Oliver Heller*).

CJEU 15 May 2011, C-543/09, (*Deutsche Telekom AG/Germany*).

Opinion A-G, CJEU 19 May 2011, C-449/09, (*Prigge*).

CJEU 12 July 2011, C-324/09, (*L'Oréal and others/eBay International AG and Others*).

CJEU 24 November 2011, C-468/10 and C-469/10, (*ASNEF and FECEMD*).

CJEU 19 April 2012, C-461/10, (*Bonnier Audio AB*).

CJEU 24 April 2012, C-571/10, (*Servet Kamberaj/Istituto per l'Edilizia sociale della Provincia autonoma di Bolzano (IPES), Giunta della Provincia autonoma di Bolzano andProvincia autonoma di Bolzano*).

CJEU 26 April 2012, C-508/10, (*European Commission/Kingdom of the Netherlands*).

CJEU 16 October 2012, C-614/10 (*European Commission/Austria*).

CJEU 15 November 2012, C-539/10 and C-550/10 (*Al-Aqsa/Council*).

CJEU 26 February 2013, C-617/10, (*Åklagaren/Hans Åkerberg Fransson*).

CJEU 26 February 2013, C-399/11, (*Melloni*).
CJEU 30 May 2013, C-342/12, (*Worten*).
Opinion A-G, CJEU 18 July 2013, C-176/12, (*Association de médiation sociale*). CJEU 26 September 2013, C-418/11 (*Texdata Software*).
CJEU 26 September 2013, C-476/11, (*HK Danmark/Experian*).
CJEU 10 October 2013, C-291/12, (*Michael Schwarz/Stadt Bochum*).
CJEU 7 November 2013, C-473/12, (*IPI*).
CJEU 12 December 2013, C-486/12 (*X*).
CJEU 8 April 2014, C-288/12 (*European Commission/Hungary)*
CJEU 8 April 2014, joined cases C-293/12, C-594/12, (*Digital Rights Ireland Ltd/Ireland, and Kärntner Landesregierung/Michael Seitlinger, Christof Tschohl and others*).
CJEU 30 April 2014, C-390/12, (*Pfleger*).
CJEU 6 May 2014, C-43/12, (*European Commission/European Parliament and Council of the European Union*).
CJEU 13 May 2014, C-131/12, (*Google Spain SL, Google Inc./AEPD, Mario Costeja González*).
CJEU 17 July 2014, C-141/12 and C-372/12 (*YS/Minister voor Immigratie, Integratie en Asiel* and *Minister voor Immigratie, Integratie en Asiel/M and S*).
CJEU 10 July 2014, C-198/13 (*Hernández*).
CJEU 11 December 2014, C-212/13, (*Ryneš*).
CJEU 5 February 2015, C-117/14, (*Nisttahuz Poclava/Ariza Toledano*).
CJEU 16 April 2015, C-446/12, C-447/12, C-448/12, C-449/12, (*W. P. Willems/Burgemeester van Nuth, H. J. Kooistra/Burgemeester van Skarsterlân, M. Roest/Burgemeester van Amsterdam, L. J. A. van Luijk/Burgemeester van Den Haag*).
CJEU 16 July 2015, C-83/14, (*CHEZ Razpredelenie Bulgaria AD/Komisia za zashtita ot diskriminatsia*).
Opinion A-G, CJEU 23 September 2015, C-362/14, (*Schrems*).
CJEU 1 October 2015, C-201/14 (*Smaranda Bara and Others*).
CJEU 1 October 2015, C-230/14, (*Weltimmo*).
CJEU 8 October 2015, C-362/14 (*Schrems*).
CJEU 17 December 2015, C-419/14 (*WebMindLicenses*).
Opinion A-G, 8 September 2016, ECLI:EU:C:2016:656, (*Opinion on the Draft Agreement between Canada and the European Union 1/15*).
Opinion CJEU (Grand Chamber), 26 July 2017, ECLI:EU:C:2017:592, (*Opinion on the*

Draft Agreement between Canada and the European Union 1/15).
CJEU 21 December 2016, C-203/15 and C-698/15 (*Tele2 Sverige/Post- och telestyrelsen* and *Secretary of State for the Home Department/Tom Watson, Peter Brice, Geoffrey Lewis*).
CJEU 29 July 2019, C-40/17 (*Fashion ID GmbH & Co. KG*).

Germany

BVerfgE 65, 1. 1983

Opinions and recommendations by the EDPB and EDPS

European Data Protection Board, formerly the Article 29 Working Party

Article 29 Working Party *Opinion 2/99 the Adequacy of the 'International Safe Harbor Principles' issued by the US Department of Commerce on 19th April 1999*, 1999, WP 19.

Article 29 Working Party *Working document ton the current state of play of the ongoing discussions between the European Commission and the United States Government concerning of the 'International Safe Harbor Principles'*, 1999, WP 23.

Article 29 Working Party *Opinion 3/1999 on the preservation of traffic data by internet service providers for law enforcement purposes*, 1999, WP 25.

Article 29 Working Party *Working document on determining the international application of EU data protection law to personal data processing on the internet by non-EU based websites*, 2002, WP 56.

Article 29 Working Party *Opinion 5/2002 on the Statement of the European Data Protection Commissioners at the International Conference in Cardiff on mandatory systematic retention of telecommunication traffic data*, 2002, WP 64.

Article 29 Working Party *Opinion 4/2005 on the Proposal for a Directive of the European Parliament and of the Council on the Retention of Data Processed in Connection with the Provision of Public Electronic Communication Services and Amending Directive 2002/58/EC (COM(2005)438 final of 21.09.2005)*, 2005, WP 113.

Article 29 Working Party *Opinion 9/2004 on a draft Framework Decision on the storage*

of data processed and retained for the purpose of providing electronic public communications services or data available in public communications networks with a view to the prevention, investigation, detection and prosecution of criminal acts, including terrorism.[Proposal presented by France, Ireland, Sweden and Great Britain (Document of the Council 8958/04 of 28 April 2004)] , 2004, WP 99.

Article 29 Working Party *Opinion 1/2008 on data protection issues related to search engines*, 2008, WP 148.

Article 29 Working Party *The Future of Privacy Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data* , 2009, WP 168.

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

Article 29 Working Party *Opinion 2/2010 on online behavioural advertising*, 2010, WP 171.

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

Article 29 Working Party *Opinion 7/2010 on European Commission's Communication on the global approach to transfers of Passenger Name Record (PNR) data to third countries*, 2010, WP 178.

Article 29 Working Party *Opinion 8/2010 on Applicable Law*, 2010, WP 179.

Article 29 Working Party *Opinion 10/2011 on the proposal for a Directive of the European Parliament and of the Council on the use of passenger name record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime*, 2011, WP 181.

Article 29 Working Party *Opinion 12/2011 on smart metering*, 2011, WP 183.

Article 29 Working Party *Opinion 13/2011 on Geolocation services on smart mobile devices*, 2011, WP 185.

Article 29 Working Party *Opinion 14/2011 on data protection issues related to the prevention of money laundering and terrorist financing*, 2011, WP 186.

Article 29 Working Party *Annex to opinion 14/2011 on data protection issues related to the prevention of money laundering and terrorist financing*, 2011, WP 186.

Article 29 Working Party *Opinion on Consent*, 2011, WP 187.

Article 29 Working Party *Opinion 16/2011 on EASA/IAB Best Practice Recommendation on Online Behavioural Advertising*, 2012, WP 188.

Article 29 Working Party *Working Document 01/2012 on epSOS*, 2012, WP 189.
Article 29 Working Party *Opinion 08/2012 providing further input on the data protection reform discussions*, 2012, WP 191.
Article 29 Working Party *Opinion 02/2012 on facial recognition in online and mobile services*, 2012, WP 192.
Article 29 Working Party *Opinion 3/2012 on developments in biometric technologies*, 2012, WP 193.
Article 29 Working Party *Recommendation 1/2012 on the Standard Application form for Approval of Binding Corporate Rules for the Transfer of Personal Data for Processing Activities*, 2012, WP 195a.
Article 29 Working Party *Opinion 05/2012 on Cloud Computing*, 2012, WP 196.
Article 29 Working Party *Opinion 06/2012 on the draft Commission Decision on the measures applicable to the notification of personal data breaches under Directive 2002/58/EC on privacy and electronic communications*, 2012, WP 197.
Article 29 Working Party *Opinion 01/2013 providing further input into the discussions on the draft Police and Criminal Justice Data Protection Directive*, 2013, WP 201.
Article 29 Working Party *Opinion 02/2013 on apps on smart devices*, 2013, WP 202.
Article 29 Working Party *Opinion on Purpose Limitation*, 2013, WP 203.
Article 29 Working Party *Opinion 05/2013 on Smart Borders*, 2013, WP 206.
Article 29 Working Party *Opinion 06/2013 on open data and public sector information ('PSI') reuse*, 2013, WP 207.
Article 29 Working Party *Opinion 07/2013 on the Data Protection Impact Assessment Template for Smart Grid and Smart Metering Systems (DPIA Template) prepared by Expert Group 2 of the Commissions Smart Grid Task Force* , 2013, WP 209.
Article 29 Working Party *Opinion 04/2014 on surveillance of electronic communications for intelligence and national security purposes*, 2014, WP 215.
Article 29 Working Party *Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC*, 2014, WP 217. Article 29 Working Party *Statement on the role of a risk-based approach in data protection legal frameworks*, 2014, WP 218.
Article 29 Working Party *Opinion 01/2014 on the application of necessity and proportionality concepts and data protection within the law enforcement sector*, 2014, WP 221.
Article 29 Working Party *Statement on Statement of the WP29 on the impact of the development of big data on the protection of individuals with regard to the processing of*

their personal data in the EU, 2014, WP 221.
Article 29 Working Party *Opinion 8/2014 on the Recent Developments on the Internet of Things*, 2014, WP 223.
Article 29 Working Party *Working Document on surveillance of electronic communications for intelligence and national security purposes*, 2014, WP 228.
Article 29 Working Party *Statement of the WP29 on automatic inter-state exchanges of personal data for tax purposes*, 2014, WP 230.
Article 29 Working Party *Opinion 03/2015 on the draft directive 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*, 2015 WP 233.
Article 29 Working Party *Opinion 2/2017 on data processing at work*, 2017 WP 249.
Article 29 Working Party *Guidelines on consent under Regulation 2016/679*, 2018. WP 259.

European Data Protection Supervisor

EDPS, 11 April 2017, *Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit*.
EDPS, 23 January 2019, *Opinion 3/2019 concerning the Questions and Answers on the interplay between the Clinical Trials Regulation (CTR) and the General Data Protection regulation (GDPR) (art. 70.1.b))*

Curriculum Vitae

RELEVANT EDUCATION

Universiteit van Amsterdam. Amsterdam — ***Graduated 2011***
Master in Law
Institute for Information Law (IViR)

Universiteit van Amsterdam. Amsterdam — ***Graduated 2009***
Bachelor in Law and Jurisprudence

Fontys Hogescholen. Tilburg — ***Graduated 2004***
Bachelor in Business Administrationt

RELEVANT WORK EXPERIENCE

Amnesty International, Amsterdam/London — 2019 – present
Senior Legal Advisor Technology and Human Rights

- Technology and Human Rights Program Manager in the Netherlands

Freelance consultancy, Utrecht — 2013 – 2018
Freelance and pro bono *privacy and data protection consultant*

- 2018 establishment of Merel Koning Consultancy

Radboud University, Nijmegen — 2012 – 2019
Researcher and teacher

- Employee at the Privacy and Identity Lab at the Institute for Computer and Information Sciences

SELECTION OF ACADEMIC PUBLICATIONS

Chapter: *Artikel 8 EVRM, Persoonsgegevens*, in *Sdu Commentaar EVRM*. The Hague: SDU 2019.

Annotation: *CJEU (Tele2), C 203/15 and C-698/15* in *European Human Right Cases* 2017/79.

Annotation: *CJEU (Schrems), C-362/14* in *European Human Right Cases* 2016/1.

Chapter: *Het recht op bescherming van persoonsgegevens in de Europese en nationale rechtsorde na Lissabon* in *Vijf jaar bindend EU-Grondrechtenhandvest*, (ed. J Gerards e.o.). Alphen aan de Rijn: Wolters Kluwer 2015.

Paper: *The ABCs of ABCs* in *Hotpets online proceedings*. Co-authors: P. Korenhof, G. Alpár and J-H. Hoepman. Privacy Enhancing Technologies Symposium: 2014.

Annotation: *CJEU (Digital Rights Ireland), C-293/12 and C-594/12* in *European Human Right Cases* 2014/140.

Article: *Publiek private samenwerking in cyberspacede gegevensvergaring* in *Computerrecht*, 2013/01.

Article: *Universele handhavingsjurisdictie in cyberspace?* Co-author: M. Hildebrandt in *Strafblad*, 2012/3