SPECIAL

Scalable Policy-awarE Linked Data arChitecture for prIvacy, trAnsparency and compLiance

Deliverable D1.2

Legal requirements for a privacy-enhancing Big Data V1

Document version: 1.0

SPECIAL DELIVERABLE D1.2

Name, title and organisation of the scientific representative of the project's coordinator:

Mr Philippe Rohou t: +33 4 97 15 53 06 f: +33 4 92 38 78 22 e: philippe.rohou@ercim.eu

GEIE ERCIM, 2004, route des Lucioles, Sophia Antipolis, 06410 Biot, France

Project website address: http://www.specialprivacy.eu/

Project	
Grant Agreement number	731601
Project acronym:	SPECIAL
Project title:	Scalable Policy-awarE Linked Data arChitecture for prIvacy, trAnsparency and compLiance
Funding Scheme:	Research & Innovation Action (RIA)
Date of latest version of DoW against which the assessment will be made:	17/10/2016
Document	
Period covered:	M1-M6
Deliverable number:	D1.2
Deliverable title	Legal requirements for a privacy enhancing Big Data V1
Contractual Date of Delivery:	30-06-2017
Actual Date of Delivery:	30-06-2017
Editor (s):	-
Author (s):	Eva Schlehahn, Harald Zwingelberg (co-author for chapters 2.2.6 and 3.3)
Reviewer (s):	Sabrina Kirrane, Piero Bonatti, Harald Zwingelberg
Participant(s):	ERCIM, WU, CeRICT, TUB, TF, DTAG, TR, PROX
Work package no.:	1
Work package title:	Use cases & Requirements
Work package leader:	CeRICT
Distribution:	PU
Version/Revision:	1.0
Draft/Final:	Final
Total number of pages (including cover):	69

Disclaimer

This document contains description of the SPECIAL project work and findings.

The authors of this document have taken any available measure in order for its content to be accurate, consistent and lawful. However, neither the project consortium as a whole nor the individual partners that implicitly or explicitly participated in the creation and publication of this document hold any responsibility for actions that might occur as a result of using its content.

This publication has been produced with the assistance of the European Union. The content of this publication is the sole responsibility of the SPECIAL consortium and can in no way be taken to reflect the views of the European Union.

The European Union is established in accordance with the Treaty on European Union (Maastricht). There are currently 28 Member States of the Union. It is based on the European Communities and the Member States cooperation in the fields of Common Foreign and Security Policy and Justice and Home Affairs. The five main institutions of the European Union are the European Parliament, the Council of Ministers, the European Commission, the Court of Justice and the Court of Auditors (http://europa.eu/).

SPECIAL has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 731601.

Table of Contents

1 Introduction

The aim of this deliverable is to identify and analyse the legal frame conditions of the European data protection framework for a lawful processing of personal data in the context of Big Data across the European Union. Thereby, the legal analysis pursues two intertwined objectives. The first is to focus on general requirements which are always applicable for all uses of personal information across the whole Big Data industry landscape. The second is to pinpoint the specific requirements for the use cases driven by the industry partners of the SPECIAL project. This is why this deliverable has two main parts: one for the general data protection requirements, and a second part focusing more on the specifics of the SPECIAL use cases. For the latter part, this deliverable will not be able to provide conclusive legal assessments, since at this stage of the project, the use cases are still in preparatory and planning phase, where still some open issues need to be considered. Those open issues which may have an impact on the legal requirements of the use cases are explicitly mentioned in that second use case part of this document. The goal is to document them here so they can be addressed further by the legal experts in the SPECIAL project together with the developing and the industry partners in order to facilitate effective, compliant and innovative use cases in a combined effort.

With the rise of the digital era and the continuous development of technology, the globally increasing of interconnectedness in digital communication networks implies an increase of data processing and involved actors as well. The concomitant automated processing of vast amounts of data is by now well-established in businesses worldwide, whereas the availability and the capabilities of Big Data technologies have significantly developed further. Consequently, the hitherto impossible analysis of unprecedented amounts of data becomes possible, evoking new economic exploitation potentials for businesses. This establishes new business models, products and services which become increasingly efficient and intelligent. Nonetheless, Big Data is also often regarded with concerns. Especially when private actors like companies collect and process personal information of individuals, the often associated comprehensive profiling of users and consumers is perceived as significantly scaling up risks of re-identification of individuals, profiling and disrupted power balances. The analysis of individual's behaviour, their social relationships, and their habits allow for a sometimes intimate knowledge of their lives. Oftentimes, those individuals are neither aware of the dimensions of the information processing, nor of what happens with this data. Usually, these persons do not know for which purposes their personal data are collected and which chances and risks come along for them. Furthermore, companies' privacy policies and other legal statements are in many cases incomprehensible to them, making an informed consent impossible.

Owed to this factual situation, and due to growing recognition of a better protection of individual's personal data needed, the European Commission triggered a reform process for the European data protection framework. From May 25th 2018, a new framework will be fully applicable, whereas for the private sector, the General Data Protection Regulation (GDPR)[1] will be the relevant data protection law in the European Union. Initially, the European Union regulated the processing of personal data with the adoption of Directive 95/46/EC[2] in 1995. However, this directive could not achieve providing legal preconditions consistently applicable across the whole Union, impeding an effective protection of individual's personal information within Europe.

[1] *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.*

[2] *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.*

With the GDPR, substantive changes have been made to improve this situation, whereas as a regulation, it will be directly binding law in all EU Member States. Furthermore, the scope of applicability has been extended to adapt the legal framework to the nature of the digital world, which is not bound by geographical barriers. Furthermore, changes were made with regard to the need for informed consent of data subjects, whereas data controllers and processors are now bound to being able to demonstrate compliance with the requirements of the GDPR. The SPECIAL project has a very strong focus on the consent and transparency requirements of the GDPR, aiming at implementing consent processes that enable a much better control of individual's over their personal data. Privacy-by-design and by default are in the focus of attention within SPECIAL, taking into account the data subjects' rights and corresponding obligations of data controllers and processors. Those were significantly enhanced by the GDPR, which has made the protection of fundamental rights more prominent than its predecessor, the Directive 95/46 EC. This deliverable will present and explain those right and obligations, such as the data subject's right to information, access, to rectification, erasure, to restriction of processing, data portability, to object, and the right not to be evaluated not exclusively on the basis of automated processing.

However, the GDPR is not the only framework relevant for the SPECIAL use cases. Since two telecommunication providers are involved as industry partners, the regulatory frame conditions for lawful processing of electronic communications are relevant to the project as well. In January 2017, the European Commission made a proposal for a directive regulating the processing of personal data and the protection of privacy in the electronic communications sector, commonly called ePrivacy Regulation (in the following for the proposal: draft ePR).[3] This draft ePR is meant to repeal the current ePrivacy Directive.[4] This draft ePR aims at complementing and particularising the GDPR, whereas the legislative process is still on-going. At the moment, the draft proposed by the commission is under review at the European Parliament and the Council, so changes are to be expected. Nonetheless, this deliverable will introduce to the application scope, the basic principles and central requirements of this legal instruments as well as the draft foresees them at the time of writing this document. Thereby, the current reception of the draft by data protection experts and the parliament will be taken into account in an attempt to anticipate the further development of the legislative process to the benefit of the SPECIAL use case planning.

[3] '*Proposal for a Regulation on Privacy and Electronic Communications*' by the European Commission.

[4] *Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).*

2 Data protection requirements V1

This chapter will describe the general legal data protection preconditions for lawful processing of personal data based upon the legal framework in the European Union. Thereby, it is important to note that by May 2018, the European data protection reform will be applicable.

In January 2012, the European Commission triggered a legislative reform process to harmonise the fragmented legal data protection framework within the European Union.[5] This reform resulted in the adoption of a directive on data protection and the sector-focused directive for the area of criminal offences which both came into force on April 27th 2016. These are:

- *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation),*[6]
- *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.*[7]

Since the SPECIAL project runtime exceeds May 2018, the project is very much focused on an early adaption of the new legal framework, whereas the GDPR will be relevant for the project work. Owed to this situation, this chapter has its primary focus on the future law while the currently applicable framework (until May 2018) will be covered only briefly.

2.1 Current legal framework and European data protection reform

The current legal framework for personal data protection in Europe is founded on the fundamental rights to respect for private and family life and to the protection of personal data.[8] With its Articles 7 and 8, the Charter of Fundamental Rights of the European Union (EUFRCh) distinguishes between the terms '*right to privacy*' and '*right to data protection*'. However, both fundamental rights are embraced in the broad term of 'private life' as manifested in the European Charter of Human Rights (ECHR). Therefore, these two core documents assume the personal information of individuals as being in need of specific protection. In the context of fundamental rights, the European Union aimed at ensuring the protection of personal data with its adoption of Directive 95/46/EC in 1995.[9]

[5] Cf. COM (2012) 9 final, titled '*Safeguarding Privacy in a Connected World - A European Data Protection Framework for the 21st Century*'.

[6] The General Data Protection Regulation (EU) 2016/679 is the main framework directly applicable in the EU member states. It is the main framework relevant for the private sector and in the following abbreviated as **GDPR.**

[7] In contrast to the GDPR, the regulatory instrument for the police and justice sectors comes in form of a directive which still needs the transfer into correlating national law by the European Member States. It is in the following abbreviated as **Directive (EU) 2016/680**.

[8] See Art. 7, 8 Charter of Fundamental Rights of the European Union (EUFRCh) and Art. 8 Convention for the Protection of Human Rights and Fundamental Freedoms (also known as European Convention on Human rights, ECHR).

[9] *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*.

At the time of writing this document, this Directive 95/46/EC is the current foundation of the applicable data protection framework in Europe, together with the corresponding national data protection laws adopted in the EU Member States. Furthermore, for the privacy of electronic communications, the current rules for lawful processing are provided by the ePrivacy Directive.[10] Common to all data protection legislation is the focus on '*protecting the fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.'*[11] The European Member States bound to transfer the minimum set of obligations into their national data protection laws..

This approach to personal data protection led to a rather fragmented regulatory framework, with numerous differences inherent in these aforementioned national laws, causing great legal uncertainty especially with regard to cross-border processing and data transfers of entities both from private and public sector entities.

The Treaty of Lisbon laid the ground for profound changes to this situation in 2009 by making the EU Charter of Fundamental Rights[12] binding to the EU Member States and giving the Court of Justice of the European Union (CJEU) enforcement competence. In this context, it was important that the European Parliament and the Council were mandated by Article 16 (1) of the Treaty of the Functioning of the European Union (TFEU) to lay down rules for the protection of personal data in the areas of freedom, justice and security, basically for the law enforcement and criminal justice sector(s). So the changes driven by the Treaty of Lisbon made it possible for the very first time to adopt much more functional and comprehensive rules for lawful personal data processing activities for the European Union.

> Therefore, the European Commission, the Parliament and the Council began to address the shortcomings of the current data protection framework and prepared for a reform process. The main objectives were to give answers to a globalized and increasingly digitalized world, to enhance trust in digital services and security by a high protection level for the privacy of the users of electronic (communication) services, and to achieve a level playing field for all market participants, for example by giving individuals more control of their personal data.[13]

Both the GDPR, as well as Directive (EU) 2016/680 entered into force and become applicable by May 25th 2018. However, the reform process is not yet complete. For electronic communications, there will be an additional framework intended to be in force and applicable by May 2018 as well, the so-called ePrivacy Regulation. At the time of writing this deliverable, this regulation is still underway in the legislative process. This regulation will repeal the current ePrivacy Directive[14] and as foreseeable by the current draft, it will expand the application to e.g. Over-The-Top service providers in addition to traditional telecom operators, effectively covering most internet-based services. The current draft[15] of the ePrivacy Regulation will most likely be subjected to relevant changes due to wide-ranged criticism by relevant stakeholders and the data protection community, such as from the

[10] *Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).*

[11] See for example Art. 1 paragraph 1 Directive 95/96/EC.

[12] Charter of Fundamental Rights of the European Union, OJ C 364, 18.12.2000, p. 1–22.

[13] Cf. the Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: '*Safeguarding Privacy in a Connected World - A European Data Protection Framework for the 21st Century*', pages 4, 7, and 10 ff.

[14] *Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)*.

[15] The '*Proposal for a Regulation on Privacy and Electronic Communications*' as made by the European Commission in early 2017 is available at: https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-privacy-and-electronic-communications

Article 29 Working Party[16] and the European Data Protection Supervisor Giovanni Buttarelli. Core aspects addressed by the criticism were vagueness of the regulation's scope definition, weaker rules related to information obligations about security risks and data breaches. Further, it misses the focus on aspects of privacy by design and by default in comparison to the GDPR. In consequence, the current draft was commented widely as lacking consistency with requirements stipulated as basis protection by the GDPR.[17]

As the domain of electronic communications plays a significant role for the SPECIAL project's use cases, it seems advisable to closely observe the legislative process for the future ePrivacy Regulation (see also chapter 2.3.8).

2.2 General Data Protection Regulation (GDPR)

This chapter presents the preconditions for the application of the GDPR. Furthermore, it explores under which basic principles and core preconditions a lawful collection and processing of personal data is possible.

2.2.1 Application scope

The application scope of the GDPR is defined both in the context of material and of territorial scope.

(a) Material scope

The material scope is defined by Article 2 GDPR, which focuses on 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.*'

Therefore, the first question to be addressed is whether personal data is concerned, whereas according to paragraph 2 of Article 2, some cases of personal data processing are excluded from the application scope, such as processing of personal data by a natural person in the course of a purely personal or household activity, for national security, for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security. Moreover, since the upcoming ePrivacy Regulation will complement the GDPR and be *lex specialis* (meaning primarily and exclusively applicable) to it once personal data are concerned, the processing of personal data in the context of electronic communications is excluded as well.

In the GDPR, '*personal data*' and '*data subject*' are defined in Article 4 (1) as follows (highlights in bold are by the author of this document):

> *(1) 'personal data' means any information relating to an **identified or identifiable natural person** ('data subject'); an identifiable natural person is one who can be **identified, directly or indirectly**, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;*

[16] The Article 29 Working Party was set up on account of Article 29 EU Data Protection Directive 95/46/EC, which demands the formation of a working group on the Protection of individuals with regard to the processing of personal data. It functions as an independent advisory group counselling the European Commission in respect to data protection and privacy aspects.

[17] See the Article 29 Working Party: '*Opinion 01/2017 on the Proposed Regulation for the ePrivacy Regulation (2002/58/EC)*', adopted on 4 April 2017, WP247, pages 3 and 24. Furthermore, see the '*Opinion 6/2017 EDPS Opinion on the Proposal for a Regulation on Privacy and Electronic Communications (ePrivacy Regulation)*', April 24th 2017, pages 3, 12 ff., 19, 22 f., and 34 f.

To determine precisely whether data is personal, the specific circumstances of an intended processing operation must be taken into account with all possible complexities and factual impact on a potential data subject.

Recital 26 GDPR aims at clarifying what the legislators envisioned as being personal information. Thereby, a focus lies on the core aspect of identifiability (again, bold highlights added):

> '*The principles of data protection should apply to* ***any information concerning an identified or identifiable natural person****. Personal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information should be considered to be information on an identifiable natural person. To determine whether a natural person is identifiable,* ***account should be taken of all the means reasonably likely to be used****, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of* ***all objective factors, such as the costs of and the amount of time required for identification****, taking into consideration the* ***available technology at the time of the processing and technological developments***.'

This recital makes it more clear that not just the legal, but also the factual and especially the technical means are of relevance for the assessment how likely it seems that an individual could be (re-)identified. Moreover, not only the means of the controller are significant, but also the reasonably likely to be used means of third parties ('[…] *either by the controller or by another person […]')*.

These viewpoints closely correspond with the perspective of the Court of Justice of the European union (CJEU), which in its judgement C−582/14 of 19th October 2016 states that dynamic IP-addresses could be personal data because '*it is not required that all the information enabling the identification of the data subject must be in the hands of one person*' and that '*a means likely reasonably to be used to identify the data subject […] would not be the case if the identification of the data subject was prohibited by law or practically impossible on account of the fact that it requires a disproportionate effort in terms of time, cost and man-power, so that the risk of identification appears in reality to be insignificant*.'[18] The possible means to identify a person, including information residing with a third party, must be considered for the evaluation of the possibility for a re-identification of the person irrespective of the costs. However, the costs are relevant for the evaluation of the likeliness of using this means. And only where the costs outweigh the value of the additional information gained it re-identification can be considered unlikely.This is something that might under circumstances be difficult to ascertain and needs to be looked at in each individual case and for each category of personal data intended for processing.[19]

Also taking into account considerations about available technology and foreseeable technological developments, it becomes clear that the decision whether personal data are involved it is not trivial but rather quite complex and challenging. Therefore, it may oftentimes deem advisable to assume that personal information is involved when in doubt.

In its Opinion 04/2007 on the concept of personal data, the Article 29 Working Party refers to the still currently valid European Data Protection Directive 95/46/EC and other relevant EU legal instruments. However, in comparison with the wording of the GDPR, it becomes apparent that core concepts and interpretations remain.[20] The definition of personal data consists of four criteria, which must all be satisfied to assume that personal information is involved.

---

[18] Court of Justice of the European Union, Judgement of the Court (Second Chamber) in the case C−582/14 Patrick Breyer v. Bundesrepublik Deutschland (Federal Republic of Germany), 16th October 2016, see paragraphs 43-46.

[19] Wolff, H.A.; Brink, S., '*Beck'scher Online-Kommentar Datenschutzrecht*', Art. 4 DS-GVO No. 18.

[20] Article 29 Data Protection Working Party: '*Opinion 4/2007 on the concept of personal data'*, WP 136, adopted on 20 June 2007.

These four criteria are:

- any information
- relating to
- an identified or identifiable
- natural person

'*Any information*' as a rather broad term plainly underlines the fact that in this first step, it is irrelevant which type, format or nature the information has, or if it is true, proven or false. Regardless of whether subjective information, opinions or assessments are involved and if it is a structured/unstructured database or filing system, all kinds of content, such as information about one's private and family life as well as information about one's professional or public life, is included in this notion.[21]

In a second step, the information has to relate to a data subject. Thereby, the Article 29 Working Party identified three possibilities how data can relate to an individual, namely via the **content** of the information, the **purpose** of the data processing or the **result** of the data processing. In this context, content is the easiest one since this can simply mean that the information is about who is someone, thus directly linking the information piece to a person, whereas indirect linkage is also possible. Purpose as a means to relate information to an individual '*can be considered to exist when the data are used or are likely to be used, taking into account all the circumstances surrounding the precise case, with the purpose to evaluate, treat in a certain way or influence the status or behaviour of an individual.*' Regarding the result of the processing, a relation could be made similarly, whereas it '[…] *is sufficient if the individual may be treated differently from other persons as a result of the processing of such data.*'[22]

The third criterion requires that data relate to an '*identified or identifiable*' person. Thereby, the term '*identifiable*' definitely causes more difficulties. So the aforementioned aspects regarding the means (ALL means likely to be used to identify a person, like legal, technical, costs….) play a crucial role. Moreover, once the very purpose of the processing is to (re-)identify a person, this also affects the concept of '*identifiability*'. In such cases, the Article 29 Working Party recommends that the information should be considered as relating to identifiable individuals and the processing should be subject to data protection rules.[23] Also, the enrichment and combination of several pieces of information with the potential to single out an individual due to unique characteristics can make a person identifiable; even if the information pieces themselves alone are on a rather high, categorical level (e.g. age category, regional origin, etc.).[24]

The last criterion is that the information relates to a '*natural person*'. This term is quite self-explanatory and synonymous with the notion of 'living individual', whereas it must be kept in mind that even objects or legal persons might relate to natural persons, for example in cases of *'corporate e-mail, which is normally used by a certain employee, or that of information about a small business which may describe the behaviour of its owner.'*[25] Similarly, the Article 29 Working Party issued a statement in another document that information about a car or vessel, such as tracking or monitoring data, can also constitute personal information about the driver or the owner.[26]

In cases where those criteria are not met, the data in question must be considered anonymous and not falling within the application scope of the GDPR. Anonymity is not explicitly defined in the GDPR,

[21] Ibidem, WP 136, pp. 6 f.
[22] Ibidem, WP 136, pp. 9 ff.
[23] Ibidem, WP 136, p. 16.
[24] Ibidem, WP 136, p. 13.
[25] Ibidem, WP 136, p. 23.
[26] Article 29 Data Protection Working Party: Letter to the Commissioner for Home Affairs Ms. Cecilia Malmström regarding the Proposal for a Regulation establishing the European Border Surveillance System, *2012,* p. 2.

but Recital (26) GDPR addresses the applicability of the regulation and states that '*The principles of data protection should therefore not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to data rendered anonymous in such a manner that the data subject is no longer identifiable.'* Therefore, this recital provides a definition with '*identifiability*' as the paramount element. An element, which is already well-known in data protection practice and research and has been subject to legal and technical research work for quite some time. Already in 2014, the Article 29 Data Protection Working Party published an opinion on anonymization techniques, thereby addressing the issue of identifiability. In order to investigate what must be done to eliminate the (re-)identifiability of an individual, the opinion focuses on existing anonymization techniques, tries to assess them from data protection law perspective, and makes recommendations for their practical use.[27]

In this context, the Article 29 Working Party makes a proposal for an assessment of whether data has been effectively anonymized by focusing on the question whether those **three risks** are sufficiently eliminated:

- Singling out which corresponds to the possibility to isolate some or all records which identify an individual in the dataset;
- Linkability, which is the ability to link, at least, two records concerning the same data subject or a group of data subjects (either in the same database or in two different databases). If an attacker can establish (e.g. by means of correlation analysis) that two records are assigned to a same group of individuals but cannot single out individuals in this group, the technique provides resistance against "singling out" but not against linkability;
- Inference, which is the possibility to deduce, with significant probability, the value of an attribute from the values of a set of other attributes.[28]

To prove that these risks are sufficiently eliminated, a reasonable effort test should be conducted to check whether the controller has performed anonymization in a reasonable way. For example, identification risks still remain if a data controller would only remove directly identifying elements. In this reasonable effort test, key data protection principles like the mandatory lawfulness of data collection and processing, necessity and purpose limitation need to be taken into account as well. In this context, the Article 29WP clarifies:

> *'The controller […] should balance their anonymization effort and costs (in terms of both time and resources required) against the increasing low-cost availability of technical means to identify individuals in datasets, the increasing public availability of other datasets, and the many examples of incomplete anonymization entailing subsequent adverse, sometimes irreparable effects on data subjects'.* [29]

For the reasonable effort, also the technical procedures and measures available to anonymize personal information must be taken into account. In the following, a very brief overview of the most important approaches will be given[30]:

- **Anonymization by data deletion**

  This approach means that, any information useable for identification is intentionally deleted from the data stock to destroy the relation to the individual. For example, if a table lists several attributes linkable to persons, like their names and the years of birth, identifiability is

[27] Article 29 Working Party: '*Opinion 05/2014 on Anonymization Techniques*', WP 216, adopted on 10 April 2014.

[28] Ibidem, WP 216, p. 14.

[29] Ibidem, WP 216, p. 9.

[30] Cf. for a more in-depth presentation of those techniques: Article 29 Working Party: '*Opinion 05/2014 on Anonymization Techniques*', WP216, pages 11 ff.

given. A possibility to eliminate the identifiability could be to delete the name as an attribute in this list per se. in this case, only the years of birth would remain as information pieces in this list and are initially not relatable to a natural person. However, the weak point in this approach is the linkability of the remaining data with external information sources, depending on the context. For instance, if this list with the years of birth relates to employees of a small company, the anonymity set could be so small that some persons could be singled out and re-identified, like e.g. the young trainee or the senior partner who is much older than the rest of his colleagues. Therefore, this case could provide for a not sufficient effort of anonymizing these persons. Furthermore, there is the possibility that the selective deletion of information might negatively affect the utility of the whole data set.

- **Anonymization by generalization**

  Another approach would be to change the original data in such a way that its information value is reduced, but without changing the semantics of said data. With the example from the section above, the original data could be changed so the exact years of birth are not mentioned any more, but rather the decade of birth can be seen. Similar approaches also exist for other types of data, such as information about origin (city, region/state/continent), or varying fine-graininess relating to categories of professional occupation. Similarly as with the approach of deletion, still depends on the context whether the generalization can be sufficient to diminish the risk of re-identification despite the existence of external information sources and context knowledge.

- **Anonymization by perturbation**

  Using perturbation, data are mixed up or enriched to obfuscate the original relations. So for instance, additional data sets can be integrated into an existing table to mitigate targeted re-identification attempts. Using the above example, more birth decades are added to cover up the potentially re-identifiable individuals. This approach seems suitable for effective anonymization, but may also have significant effect on the quality and reliability of the data stock overall. Furthermore, while perturbation can be useful to counter known re-identification methods, it is less so for unforeseen approaches for which no correlating enrichment of data occurred to obfuscate the context information.

- **Anonymization by aggregation**

Using this methodology, all data sets are merged to extract results of a more general nature. Similar to the generalization approach, there is the problem that the precise information gets lost in favour of a more high-level insight. An example would be the calculation of the average year of birth of all employees of a company. For this, the sum of all years of birth would be divided by the number of employees. The result would have some insight regarding the average age of the workforce without allowing any direct inference to the specific age of an individual employee, but with the potential exception that the exact dates of the other workers would be determinable from external information sources. According to the state-of-the-art and besides the deletion of the data, aggregation can be assumed as the most secure method of anonymization because it allows for a sufficiently large anonymity set. Usually, a re-identification is realistic only under unlucky circumstances and with smaller data sets. However, it must be acknowledged that additional context information may still diminish the desired effect of this method.

- **K-anonymity**

In 1998, Samariti and Sweeney published a paper referring to the definition of k-anonymity, which basically focuses on the specification of suitable request restrictions to ensure certain characteristics of the data stock. The essential requirement for this is that a data stock needs to have a minimum *k* of not determinable data sets, which is quite similar to aggregation, but differs in terms of timing. The goal is to hinder the acquisition of information about groups with less than *k* data subjects. In case a request to a k-anonymized data set occurs, the processing must be

limited in such a way that either the k minimum must be fulfilled, or the request is denied.[31] In the research community, k-anonymity has gained some recognition. Nevertheless, its main issue is the real-world realization of the concept. So for example, the transfer of a k-anonymized data stock cannot occur in cases the recipient already has a different version of the k-anonymized data. This unfolds impact especially over time, when the observation of the data stock allows for conclusions. For example if the k-anonymity is meant to ensure that not less than two employees have the same year of birth (k=2), the context changes in case one of those employees leaves the company. Furthermore, there are some technical difficulties with the k-anonymization of a data stock consisting of more complex data formats, like images and block text. For such cases, further developed concepts have been defined, such as L-diversity[32] and T-closeness[33]. However, those concepts also have their own difficulties in technical realization.

It must be noted that all of these techniques do not provide a 100% guarantee. Rather, the Article 29 working Party clarified that in practice, the (re-)identification has to be "reasonably" impossible. Such an assessment may under circumstances be quite difficult, taking into account that over time, the risk of (re-)identification may increase due to research, tools, and computational power evolving and further developing. The Working Party emphasises that an exhaustive enumeration of circumstances when identification is definitely no longer possible cannot be made. So techniques of anonymization will remain the subject of ongoing research while it must be assumed that no technique is devoid of shortcomings per se.[34]

As for pseudonymization, such information would be considered as personal data still, but with enhanced protection for the data subject. Article 4 paragraph 5 GDPR gives the following definition (highlights in bold added by the author):

> *'pseudonymisation' means the processing of personal data in such a manner that the* ***personal data can no longer be attributed*** *to a specific data subject* ***without the use of additional information****, provided that such additional information is* ***kept separately*** *and is subject to technical and organisational measures* ***to ensure that the personal data are not attributed*** *to an identified or identifiable natural person;*

Here, the attribution to an individual's real name and the linkage probability plays a role. According to the Article 29 Working Party, pseudonymization is not an anonymization technique. Rather, pseudonymization just means that attributes (typically unique attributes e.g. identification number or name) are replaced by another kind of identifier (e.g. a nickname, a number or the like).[35] The document (as table or the like) listing identifiers and the related individuals (respectively the information relatable to those persons, e.g. name, email address, telephone number) functions as code book which is not to be disclosed by the controller to data processors and third parties. Other encoding methods with various types of identifiers may exist, as well as multilevel (repeated) encoding of data to make re-identification more difficult. However, regardless of which approaches have been used, a re-identification may still be possible with the enrichment of the pseudonymized data by additional publicly available datasets.[36]

---

[31] Samarati, P., Sweeney, L.: '*Protecting Privacy when disclosing information: k-Anonymity and its enforcement thourgh generalization and Suppression*', Proceedings of the IEEE Symposium on Research in Security and Privacy (S&P). May 1998, Oakland, CA.

[32] Machanavajjhalaet, A. et al.: '*l-diversity: Privacy beyond k-anonymity*', (TKDD), Vol. 1, 2007, article no. 3.

[33] Li, N.; Li, T.; Venkatasubramanian, S: 't-*Closeness: Privacy Beyond k-Anonymity and l-Diversity*', ICDE Vol. 7, 2007, pp. 106-115.

[34] Ibidem footnote 30, WP216, p. 12.

[35] Ibidem footnote 30, WP216, p. 20.

[36] Barbaro, M.; Zeller, T.: '*A Face Is Exposed for AOL Searcher No. 4417749*', The New York Times, 2006.

Consequently, the Article 29 Working Party assumes the following re-identification risks in the context of pseudonymization:

- Singling out might still be possible, as the individual is still identified by the allocation of a unique attribute (= the pseudonymized attribute).
- Linkability may appear between records using the same pseudonymized attribute.
- Inference may emerge with regards to the real identity of a data subject within the data set or across different data stocks in case the same pseudonymized attribute is used for an individual, or if pseudonyms are self-explanatory.[37]

When addressing those risks sufficiently, an effective use of pseudonymization reduces the linkability of a dataset with the original identity of a data subject. Therefore, in cases where is can be applied, it enhances the level of security and data protection.

Once it is clarified whether personal data is involved, the next question is whether '*processing*' of this data is concerned. Article 4 (2) GDPR defines the term as follows (bold highlights added):

> *(2) 'processing' means **any operation or set of operations which is performed on personal data** or on sets of personal data, **whether or not by automated means**, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;*

From this definition, it is clear that the whole lifecycle of personal data treatment is captured by the application scope, from the very moment of collection. It does not matter if the processing operation is offline, paper-based or digital by using information technology. Furthermore, the list is not conclusive as to keep the legal framework technologically neutral in anticipation of novel technological approaches to treat personal information.

(b) Territorial scope

Article 3 GDPR regulates the territorial scope of the regulation. The legislators had the goal to specifically address cross-border and international data processing in order to create the same rules for all data controllers and processors operating within the European market. According to Article 3 (1) GDPR, the legal framework applies once a data controller or processor has an establishment within the European Union, regardless of whether the processing takes place in the Union or not. According to Article 4 (16) GDPR, which provides a definition of the main establishment of a controller, the crucial question is where the decisions regarding purposes and means of the processing of personal data are taken. Already for the territorial scope of the still current Directive 95/46 EC, [38] the CJEU clarified that the notion of '*establishment*' has to be interpreted broadly in such a fashion that if the controller exercises a minimal '*degree of stability of the arrangements and the effective exercise of activities*' in the territory of a Member State, an establishment in that Member State can be assumed. Thereby, to ensure '*effective and complete protection of the right to privacy and in avoiding any circumvention of national rules*', particularly when the offer of services through the internet is concerned, the respective requirements should not be set too high so '*any real and effective activity — even a minimal one*' of the controller may suffice.[39] In another ruling, the CJEU has taken the same stance, stating that '*Directive 95/46 does not require the processing of personal*

[37] Ibidem footnote 30, WP216, p. 21.

[38] Cf. hereto Article 4 para. 1 (a) of Directive 95/46 EC: '*1. Each Member State shall apply the national provisions it adopts pursuant to this Directive to the processing of personal data where: (a) the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State […]*'.

[39] CJEU judgement of 1 October 2015 in case C-230/14 *Weltimmo s.r.o. v Nemzeti Adatvédelmi és Információszabadság Hatóság ('Weltimmo')*, para. 29 ff.

data in question to be carried out 'by' the establishment concerned itself, but only that it be carried out 'in the context of the activities' of the establishment.'[40] With the data protection reform, the legislators took these decisions into account by clarifying in Recital 22 GDPR that the '*legal form of such arrangements, whether through a branch or a subsidiary with a legal personality, is not the determining factor in that respect*'. So with the upcoming new legal framework having the same terminology of '*establishment*', this means that a controller or processor have to comply once they have even minimal activity within the Union territory through a stable arrangement and with links to activities of the establishment carrying out the processing. But Article 3 GDPR also brings in one new aspect: Regardless of physical location, the GDPR is applicable once data subjects are located in the EU and goods and services are offered to data them or the processing is intended to monitor their behaviour. This is especially relevant in the context of goods and services offered through international networks such as the internet. This way, the legislators took account of the rapid technological development and of globalization and tried to find ways to hinder circumvention of rules designed to ensure the protection of individuals. Thereby, in Recital 23 of the GDPR, it is clarified that for those goods and services its does not matter whether they are '*connected to a payment*'. Rather, factors like language and currency used, as well as the direct offering to individuals in the union play a role. So for example, if goods and services offered via the internet are offered in German or Italian language, or payment is demanded in Euro, it can be assumed that EU citizens are targeted as customers.

2.2.2 Controller and processor

Article 4 (7) GDPR provides a definition for a data controller, the entity legally responsible for the personal data collection and processing (bold highlights added):

> '*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 processing*** *of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;*'

Therefore, the entity making the decisions over which data is being collected and why is to be seen as the controller. Thereby, it is important to note that the GDPR explicitly allows joint controllership ('*alone or jointly with others*') where under such circumstances, several entities can be responsible. The determination who is controller must be made taking into account the real circumstances of the individual case and the factual influence of the entity in question.[41] Consequently, not all recipients of personal data are controllers. Rather, in cases where another entity determines purposes and means of the processing, the recipient could be a processor. Article 4 para. 8 GDPR defines the term '*processor*' as well, stating:

> ''*processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;*'

Thereby, it is notable that the GDPR obliges both, the controller, as well as the processor with the protection of personal information. Nonetheless, when a processor agrees to process data on behalf of the controller the following is required:

- A precise allocation of responsibilities,
- managerial authority of the controller and

[40] CJEU judgement of 13 May 2014 in the case C-131/12 *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González ('Google Spain')*, para. 52.

[41] Article 29 Working Party, '*Opinion 1/2010 on the concepts of "controller" and "processor"*', WP 169, adopted on 16 February 2010, page 11.

- based on this authority, the processor is bound to the instructions of the controller.

Any processing on behalf of the controller must be governed by a contract or legal act under Union or Member State law. The European Commission or a European supervisory authority may lay down standard contract causes to be used. What is new is that a contract can now also be in electronic form, not just in writing (Art. 28 para. 8 + 9 GDPR). Moreover, these rules also apply due to the broad territorial scope of the GDPR (Art. 3 para. 2) to cases where a controller or processor is located outside of the EU. If the processor wants to involve a sub-processor, the controller needs to agree first in written form (Art. 28 para 2 + 4). Then, the processor needs to oblige the sub-processor with the same duties corresponding to those imposed on him in his agreement with the controller.

In case of an infringement of the GDPR, the data subject can turn to the controller and the processor(s) liable to demand compensation for material or non-material damage suffered (Art. 82 para 1 + 2 GDPR). This can under circumstances mean that the controller and the processor can be liable jointly, whereas the data subject is free to decide to hold one of them responsible for the entire damage to receive effective compensation (para 4). In turn a controller or processor being held liable for the entire amount can claim back part of the compensation from the other responsible controller(s) and processor(s) (Art. 82 para. 5).

2.2.3 Basic principles

Despite being a completely new legal framework, core principles of the current Directive 95/46/EC remain. These address aspects like transparency, purpose limitation and data minimisation, accuracy, storage limitation based on necessity, integrity and confidentiality, and accountability.

Article 5 paragraph 1 GDPR presents those basic principles to enable lawful personal data processing. It says (highlights in bold by the author):

> '*Personal data shall be:*
>
> > *(a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and* ***transparency****');*
> >
> > *(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; 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 ('****purpose limitation****');*
> >
> > *(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('****data minimisation****');*
> >
> > *(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('****accuracy****');*
> >
> > *(e) 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; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('****storage limitation****');*
> >
> > *(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against*

*accidental loss, destruction or damage, using appropriate technical or organisational measures (‘**integrity and confidentiality**’).*

*2. The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 (‘**accountability**’).’*

In contrast to the Directive 95/46 EC, a violation of these principles embedded in the GDPR can now be sanctioned with much more impact on data controllers. Article 83 GDPR manifests the general conditions for imposing administrative fines, whereby under para. 5 (a), with reference to Article 5, infringements on the basic principles can lead to fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, depending on which amount is higher.

(a) Transparency

Transparency is the verification of data protection compliance with reasonable effort. It is a key data protection principle in favour of the data subject, which shall ensure the lawfulness and fairness of the processing. This principle is also linked to the right to a fair trial, as defined by Article 6 of the European Convention for the Protection of Human Rights and Fundamental Freedoms and Article 47 of the Charter of Fundamental Rights. So when taking the fundamental rights underpinning of the data protection framework into account, the perspective of the data subject is paramount.[42] In November 2015, the European Data Protection Supervisor Giovanni Buttarelli issued an opinion addressing the lack of transparency that prevails often in Big Data contexts. Thereby, he clarified that ‘*Individuals cannot efficiently exercise control over their data and provide meaningful consent in cases where such consent is required. This is all the more so as the precise future purposes of any secondary use of the data may not be known when data is obtained: in this situation, controllers may be unable or reluctant to tell individuals what is likely to happen to their data and to obtain their consent when required.*’

Ideally, transparency covers the complete lifecycle of the data, from the moment of collection onwards to the stages of processing, storage and deletion. Sufficient transparency would give adequate insight into the purposes and means of a data processing, enabling the data subject to learn what personal data is being processed, when, and by whom for which reason. Nonetheless, transparency is an important element for data controllers, processors, and supervisory authorities as well. It is rather explicit and also inherent in many different articles of the GDPR, for example in:

- Art. 12 (Transparent information, communication and modalities for the exercise of the rights of the data subject)
- Art. 13 (Information to be provided where personal data are collected from the data subject)
- Art. 14 (Information to be provided where personal data have not been obtained from the data subject)
- Art. 15 (Right of access by the data subject)
- Art. 30 (Records of processing activities)

In terms of concrete technical and organisational measures, transparency can be achieved through either paper-based or digital documentation of technical and organisational systems and processes, data flows, access authorisation concepts, and the factual accesses to the data. In this context, monitoring systems and logs support transparency as they allow either real-time or ex-post knowledge about changes on the personal information, including additions, modifications, and deletions. Records of processing activities (the above mentioned paper-based or digital

[42] Opinion 7/2015, ‘*Meeting the challenges of big data*’, 19 November 2015, page 8.

documentations) are designed to reliably provide up to date, complete and accurate descriptions of the data, the processing operations, and the respective executing systems. This way, audit-proof controllability, verifiability and assessability of the processing operation at any time is possible. In the context of digital processing operations, there is a range of technical as well as organisational measures which are fairly suitable to establish transparency. Some not conclusive examples for transparency-enhancing technical and organisational measures[43] are:

- Verification of data sources
- Documentation of IT processes
- Documentation of institutional procedures
- Documentation of testing
- Documentation of (related) contracts
- Logging of accesses & changes of the data
- Versioning of different prototypes/systems
- Track-keeping of data, especially data essential for decision-making
- Documentation of valid, informed and free consent, or its refusal or withdrawal

In general, the question how to facilitate transparency is usually context-dependent, meaning that it must always be tailored to the specific factual deployment circumstances of the processing operation.[44] This encompasses three dimensions, namely the technical, organisational and regulatory dimensions relating to the processing in order to be fully comprehensive.[45] Therefore, it is important to clarify which of these are needed in the SPECIAL use cases, especially with regard to consent management and usability.

(b) Purpose limitation

First and foremost, purpose limitation expresses a limitation of personal data collection and storage and formulates rules on the use of personal data for specific legitimate purposes. According to Article 5 para 1 (b) of the GDPR, purpose limitation has as core element that data must be collected only for specified, explicit and legitimate purposes (purpose specification).

Such specification of a purpose guarantees the transparency of data collection, processing and use of personal data for the data subject.[46] A processing operation going beyond this purpose is usually without consent or other legal ground and as such is not permitted. As a consequence, the purpose of the processing must be determined already prior to the collection of the information (cf. for example Art. 6 para.1 (b) of the GDPR). In today's data-driven society, there are now many companies that offer services mainly focusing on data collection as a premise to provide the service in the first place, or where the core purpose is basically the profiling of the user. However, already in 2013, the Article 29 Working Party has highlighted that for an assessment of the legitimacy of a purpose, '*the nature of the underlying relationship between the controller and the data subjects,*

[43] Exemplary list under reference of the Standard Data Protection Model recommended for use in Germany: https://www.datenschutzzentrum.de/sdm/. The linked English document version is a trial version while an improved translation is currently in the works.

[44] Danezis et al.: *'Privacy and Data Protection by Design – from policy to engineering'*, 2014, chapter 4.11 p. 44 ff.

[45] Gürses, Troncoso, Diaz: *'Engineering Privacy by Design'*, 2011.

[46] Cf. for example the census decision of the German Federal Constitutional Court (in German: Volkszählungsurteil Bundesverfassungsgericht) of 15th December 1983, which basically says that a social and legal order '*in which individuals can no longer ascertain who knows what about them and when*' would not be compatible with their right to informational self-determination. A sufficient knowledge is meant to be achieved exactly by a prior and precise determination of processing purposes.

whether it be commercial or otherwise' must always be taken into account.[47] In technical terms, a limitation to specific purposes can be achieved e.g. through the adherence to the principles of necessity, data minimisation and confidentiality, with effective concepts for the separation of data and systems, and the deletion of data after the fulfilment of the processing purpose(s).

For the further processing of personal data beyond the initial purpose, Article 6 para. 4 GDPR gives a concluding list of permissible cases, which are:

- the consent of the data subject,
- the processing is based on union or Member State law constituting a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 23(1) GDPR,
- the processing is not incompatible with the initial purpose.

For the last case in a compatibility assessment, the legislator mentions specific criteria to use in such an assessment in Article 6 para. 4 (a) to (e) GDPR. These criteria are:

- Link between new purpose and initial purpose
    - Here, it plays a role how closely connected the new purpose is to the original one, for example time-wise and with regard to the circumstances of the case.
- Context of data collection
    - Here, the relationship between data subject and data controller is the main element. Influential on the assessment must be the power balance, the free will of the data subject and eventual legal obligations to provide information.
- Nature of the personal data
    - For example, it is of importance if special categories of data, for which stricter rules apply, are intended to be processed. Examples of such special data categories are information about religion, sexual orientation, philosophical or political beliefs.
- Consequences for the data subject
- This criterion focuses on the impact on the subject, while negative consequences are to be understood broader than just physical or monetary damage (for example, discrimination). The more probable it is that negative consequences happen, the more plausible it is as well to assume incompatibility.
- The existence of appropriate safeguards
- Here, the measures of encryption or pseudonymisation are mentioned as possible safeguards, while these are just examples. At this step, an attempt can be made to compensate for aspects above mentioned in this list and to minimize the risks for the data subjects.

This list is not conclusive enough to enable a more in-depth assessment based on the circumstances of the individual case. In some cases, the legislator assumes a compatibility of further processing, such as further processing for archiving purposes in the public interest, and for scientific or historical research or statistical purposes (Art. 5 para. 1 (b) sentence 2 of the GDPR). Yet, these additional purposes must also comply with Article 89 (1) of the GDPR, requiring appropriate safeguards for the rights and freedoms of the data subject are put in place.

Any further usage of the data for other purposes requires anew a legal ground, such as another contract, or further consent to be given by the data subject (see hereto chapters 2.2.4 and 2.2.5).

[47] Article 29 Working Party: '*Opinion 03/2013 on purpose limitation*', WP 203, adopted 2 April 2013, p. 20.

(c) Data minimisation

Any personal data collection must be adequate, relevant and limited to what is necessary in relation to the purposes. The necessity of the processing in relation to the purposes is closely related to the idea of the unlinkability of data. Unlinkability means that personal data should not be linked across different domains to be used for a different purpose than initially determined. Therefore, unlinkability is an enforcement of purpose limitation and necessity (including data minimisation). As for the realisation by technical and organisational measures, this could be facilitated e.g. by only selective and filtered data collection, separation of data according to its purpose-bound processing context (physically and/or virtually), access control, pre-defined retention periods, sticky policies, and the usage of pseudonymisation and anonymisation. Usually, this preconditions a clear conception of related technical work processes as well as fine-grained user role and clear data access authorisation concepts.

(d) Accuracy

According to Art. 5 para 1 (d) of the GDPR, data must be '*accurate and, where necessary, kept up to date; every reasonable step must be taken 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 principle is focused on enabling the data subject to exercise more control over the own data while this is connected to the data subject's rights, requiring under circumstances either direct or indirect, yet always effective intervenability on processing operations. In the literal sense, intervenability is the operational access to processes and data either by effective technical or organisational means, for example being able to modify or delete inaccurate personal data. This preconditions the transparency and controllability of data collection and the related processes and systems. But intervenability is important not only for the data subject. Rather, other involved entities, like providers, system users, or supervisory authorities may have an interest in being able to intervene within the scope of their roles and competences. Examples of realisation measures are system functions for the upload, modification, and deletion of data. Furthermore, the availability of the personal information is also entailed, requiring the functioning of processes and systems without deficiency, data loss and malfunctions. Therefore, data redundancy and backup concepts and the sufficient stability of the provided IT services are necessary strategies to comply as well.

(e) Storage limitation

Article 5 para. 1 (e) GDPR requires that data must be '*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*'. This principle is intertwined with purpose and necessity as well. Thereby, in Big Data contexts where data is collected from multiple and often mixed-format sources, it usually depends on the context which data categories need to be stored for a certain period of time. So for example, in relation to specific data sets, meta data collected to provide a certain service typically can be deleted much earlier (since it is not needed anymore after the service provision) than for example billing data, which must be stored much longer due to legal obligations.

(f) Integrity and confidentiality

Integrity ensures that systems fulfil the foreseen functions reliably. This preconditions that processes and systems remains intact and complete without corruption, damage or loss of personal data. Some examples for realisation measures are hash-value comparisons, backup & restore and other functionalities to enable corrective actions. The required confidentiality of personal information means that no unauthorised third party acquires knowledge of the data. For efficient access control, a clear user role concept is a precondition mandatory to decide who is allowed to see the data and

who is not. In this context, a broad view on the overall context and an expectation of various attack schemes is valuable (e.g. also taking into account IT system administrators as potential malicious insiders). Other measures to support confidentiality are the encryption of data as well as the physical security of the IT system (devices, servers, and other hardware).

(g) Accountability

Paragraph 2 of Article 5 GDPR allocates the legal responsibility to the data controller and demands that the controller must be able to demonstrate compliance with the rules laid down in the GDPR. This can be done e.g. by documenting the legal basis, the purposes and the means of a specific processing operation types, e.g. in an index of procedures describing the processing operations and the technical and organisational circumstances. Such documentation should involve:

- The categories of personal and data formats intended to be used
- The sources of these data categories
- The purposes for which it is intended be to used
- The legal ground on which the processing operation is based
- Technical systems involved (hardware, software and infrastructure)
- The processing entity's internal organisation and human resources involved when processing of data with the systems

Furthermore, technology may support the demonstration of compliance in various ways, for example by providing means to prove that the system is functioning properly, creating an audit trail with logging and a data model/ontology (which conceptually, logically and physically describe structure and flow of the information and inferences), enabling a clear re-traceability which data sets were used for which analytical processes and how the corresponding analytical results were generated (data, process and analytical provenance). For each process, specific roles of involved actors must be determined to allocate the legal responsibilities (i.e. accountability). This is typically done by defining specified and assigned as roles in a comprehensive role concept. Such a role concept is a core precondition to determine which of the participating organisational instances has to actively ensure the legitimacy of a data processing procedure. This is especially important in more complex organisational structures, whereby it is possible to classify either whole organisation-wide processes, or independent sub-processes.

2.2.4 Legal ground

Article 6 GDPR manifests the initial preconditions of lawful personal data processing under the regime of the regulation. Quoting from paragraph (1) of this article (bold highlights added):

> *1. Processing shall be lawful only if and to the extent that at least one of the following applies:*
>
> > *(a) the data subject has given **consent** to the processing of his or her personal data for one or more specific purposes;*
> >
> > *(b) processing is **necessary for the performance of a contract** to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;*
> >
> > *(c) processing is **necessary for compliance with a legal obligation** to which the controller is subject;*
> >
> > *(d) processing is **necessary in order to protect the vital interests of the data subject** or of another natural person;*
> >
> > *(e) processing is **necessary for the performance of a task carried out in the public interest or in the exercise of official authority** vested in the controller;*
> >
> > *(f) 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, in particular where the data subject is a child.*

Therefore, the processing of personal data is in principle always prohibited, unless it is based on one or more of the legal grounds listed above.

- In the context of the SPECIAL project, it will be investigated primarily whether technical means can be used to support efficient and compliant consent management, including consent requests, grants, withdrawal and possibly, partial withdrawals. Therefore, the specific preconditions for valid consent will be addressed in-depth in a dedicated follow-up chapter to support the project in identifying the non-functional and functional requirements which need to be implemented for the project's use cases.
- Other legal grounds, such as legal obligations and legitimate interests of the data controller or third parties not overridden by the interests or fundamental rights or freedoms of data subjects, will be explored in the project as well.

In addition, it is important to keep in mind that the GDPR foresees special categories of personal data for which even more restrictive conditions apply. Those special categories are regulated by Article 9 of the GDPR, which has some additions to the special categories of personal data as they were known in the Directive 95/46 EC. According to the GDPR, special categories of personal data concerning an individual (data subject) are:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Genetic data
- Biometric data for the purpose of uniquely identify a natural person

- Information about health or sex life, and sexual orientation[48]

Also for this data, the principle of processing prohibition with permission reservation persists. This means that the processing of such special categories of data is prohibited, unless there is an explicit legal permission. Such information may only be processed under strict preconditions which are laid down in Article 9 (2) of the GDPR. Examples for such justifications are:

- Explicit consent of the data subject for one or more specified purposes
- A specific law allowing it based on Union or National law
- Data is necessary to protect the vital interests of the data subject or of another natural person
- Such processing related to data already made public by the data subject

This list above is not conclusive, but exemplary only. In general, it can be said that the processing of those above mentioned special categories of personal data requires a much stricter consideration of the necessity principle. This is due to the sensitive nature of such information and to ensure such data are only processed when absolutely no other options are available. Depending on the context, the processing of such data could increase the need for additional protective technical and organisational measures (anonymization or pseudonymization).

In the list of special categories of personal data, location data is not mentioned. Nonetheless, the processing of location data is sometimes seen as high risk processing since sensitive information related to the special data categories mentioned in Article 9 GDPR may eventually be derived indirectly. Therefore, in the context of location data, it deems advisable to treat location information like a special category of personal data. Particular care should be taken to deploy sufficient technical and organisational measures to achieve an adequate level of protection, including a prior data protection impact assessment.[49]

[48] Cf. Article 9 para. 1 GDPR.

[49] Article 29 Working Party, '*Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679*', WP 248, adopted on 4 April 2017, p. 8.

2.2.5 Consent

Consent, when given under the fulfilment of all preconditions of the GDPR, can be a valid basis and legal ground for the processing of personal information. The legal preconditions for consent are laid down in Art. 4 (11) and 7 of the GDPR, requiring valid consent to be

- freely given, specific, informed and unambiguous (for one or more specific purposes)
- possible to withdraw at any time
- a statement or clear affirmative action of data subject expressing agreement

The existence of valid consent must be **demonstrable** by the data controller (accountability).

(a) Freely given, specific, informed and unambiguous (for one or more specific purposes)

Free is the granting of consent only when there is **no coupling with the performance of a contract, including the provision of a service**, which is conditional on consent when the data is not necessary for the performance of that contract. Art. 7 (4) GDPR clarifies that (bold highlights added):

> '*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.*'

In this context, the relationship between data subject and data controller plays an important role. With the European data protection reform, the legislators intended to strike a better balance between those two actors and give the data subject more leverage against the market power of companies and especially against the coercive power of public authorities (cf. Recital 43 GDPR). In that context, the Article 29 Working Party stated already in 2011:

> '*Consent can only be valid if the data subject is able to exercise a real choice, and there is no risk of deception, intimidation, coercion or significant negative consequences if he/she does not consent.*'[50]

Especially in the context of an employer-employee relationship, the question of freedom of choice may be quite difficult to answer. Where the personal information is not a condition for the employment itself, the worker would only in theory be able to refuse consent, but in practice would strongly feel compelled to give consent to avoid losing their job.[51]

When data collection and processing is intended for multiple purposes, it is necessary to ensure that consent is covering all of these purposes (cf. Recital 32 GDPR). However, the question is whether all kinds of purposes can be addressed in one single consent form, broadly formulated as pre-emptively covering future business models of the data controller. Therein, Recital 43 GDPR casts doubt on this approach, stating:

> '*Consent is presumed not to be freely given if it does not allow separate consent to be given to different personal data processing operations despite it being appropriate in the individual case, or if the performance of a contract, including the provision of a service, is dependent on the consent despite such consent not being necessary for such performance.*'

[50] Article 29 Working Party, '*Opinion 15/2011 on the definition of consent*', WP 187, adopted on 13 July 2011, p. 12.

[51] Ibidem, WP 187, page 13 f.

Consequently, **globalized, generic consent for multiple vague purposes may be assumed as not freely given**. So naturally, the difficulty lies in the question whether separate consent is appropriate. When assessing the need for several, broken down consent requests, it must be kept in mind that the perspective of the data subject is paramount since the preconditions of the GDPR set the primary focus on the protection of the rights and freedoms of the data subject, Art. para. 1 (1) GDPR.

(b) Withdrawal of consent

Furthermore, Art. 7 para. 3 GDPR demands that **consent can be withdrawn at any time**, and the **withdrawal must be as easy as giving consent**. This is to prevent higher burdens for withdrawal, such as when giving consent would be with just one click online, but the withdrawal is required by the controller in written form or the like (which is thus not allowed). Art. 21 (5) GDPR states that **automated procedures to enable the data subject to exercise the right to object are possible**. This is something that would also be interesting to explore in the context of the SPECIAL project (Privacy by default compliance). The data subject must receive **information about the possibility of consent withdrawal prior to giving consent**. Therefore, it is advisable to notify the data subject that withdrawal is possible at any time at the same time as the consent request.

(c) Statement or clear affirmative action of data subject

This means consent does not necessarily need to come in written form. Instead, it can be given in a written statement (including electronic means) as well as by oral means. Recital 32 GDPR gives some examples, such as:

- ticking a box when visiting an internet website,
- choosing technical settings for information society services or
- another statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of his or her personal data

However, there are some examples what is not sufficient:

- silence,
- pre-ticked boxes or
- inactivity

These will not fulfil the conditions of valid consent. Furthermore, Recital 32 recommends that if the data subject's consent is to be given following a **request by electronic means,** such a request must be:

- clear,
- concise and
- not unnecessarily disruptive to the use of the service for which it is provided.

Art. 7 para. 2 says that when consent has to be given in a written declaration which also concerns other matters (e.g. a contract for the provision of a service), the request for the consent must be

- presented in a manner which is **clearly distinguishable from the other matters**
  - meaning that consent should not be 'hidden' somewhere in large contractual texts
- in **an intelligible** and **easily accessible** form, using **clear and plain language**
  - meaning that a consent request should not consist of pages-long 'legalese', rather be easy to understand for the average consumer.

Art. 7 para. 2 sentence 3 makes clear that any consent given on the basis of a request not complying with these preconditions is not binding (i.e. invalid) and may lead to the imposing of fines by a data protection supervisory authority.

(d) Stricter rules for special categories of personal data and consent of children

In cases where **special categories of personal data** (in the sense of Article 9 para. 1 of the GDPR, see chapter 2.2.1 above) are intended for collection, the consent must be made '*explicit*', see Art. 9 para. 2 (a). This is a strong argument for a very clear wording for what the consent is required and for a written and well-documented form. Furthermore, if consent from minors is requested, Article 8 GDPR says that **consent can be obtained when the child is at least 16 years old**. **When the child is younger**, the processing can only be lawful if the **consent is given or authorised by the holder of parental responsibility over the child**. In such cases, the controller must make an extra effort to verify the valid obtainment of the consent.

2.2.6 Data subject's rights

The General Data Protection Regulation, being focused on the protection of the rights and freedoms of individuals, demands from the controllers and processors of personal data that they make the exercise of data subject's rights possible. These are specifically laid down in the Articles 12 –22 GDPR.

(a) Overview of data subject rights

The data subject rights are:

- Transparent communication (Art. 12 GDPR)
- Information regarding the identity of the controller and the processing itself. This includes the means and purposes of the processing, whereas the law distinguishes between two cases:
  - Personal data are collected from the data subject (Art. 13 GDPR)
  - Personal data have not been obtained from the data subject (Art. 14 GDPR)
- Right of access (Art. 15 GDPR)
- Right to rectification of inaccurate data (Art. 16 GDPR)
- Right to erasure, '*right to be forgotten*' (Art. 17 GDPR)
- Right to restriction of processing (Art. 18 GDPR)
- Right to receive a notification from the controller regarding rectification or erasure of personal data or restriction of processing (Art. 19 GDPR)
- Right to data portability (Art. 20 GDPR)
- Right to object (Art. 21 GDPR)
- Protection against automated decision-making, including profiling (Art. 22 GDPR)

Over the course of the project's runtime, SPECIALwill explore more in-depth in which ways technology can support the exercise of these rights, not just the rights to transparent communication and to information. Thereby, the objective of the project's research is to identify how for example a layered approach[52] as part of consent requests and the planned dashboard can provide effective and sufficient functionalities for the users. This includes functionalities for data subjects to access and

[52] E.g. as proposed by the Article 29 Working Party in its '*Opinion 10/2004 on More Harmonised Information Provisions*', adopted 25th November 2004, WP100, p. 6 et. seq.

manage their own personal data (e.g. to rectify incorrect information, to give/withdraw consent - even partially for specific purposes only, or to restrict processing themselves directly). The legal obligation of the controller to facilitate the transparent communication and information towards the data subject plays an important role in the SPECIAL project. The research and development work is to a large part aimed at technological support of user consent acquisition, at creating a dashboard with feedback and control features as well as establishing auditability to enhance transparency for data subjects and controllers alike as well as for compliance verification, e.g. in relation to control organs such as data protection authorities. Given the project's focus on transparent communication and information obligations of the controller, this will be elaborated more in-depth in the following subsections. Other data subject rights will be examined as well as part of the legal contributions to the project's use cases.

(b) Transparent communication and information

For all communication with the data subject, Art. 12 para. 1 GDPR demands that:

> '*1. The controller shall take appropriate measures to provide **any information** […] relating to processing to the data subject in a **concise, transparent, intelligible and easily accessible form, using clear and plain language**, in particular for any information addressed specifically to a child. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means.'*

These requirements closely correspond with the recommendations the legislator made for consent requests in general in Recital 32 GDPR (see above chapter 2.2.5).

- Therefore, it has to be explored which technical means generally are possible and in particular in the project use cases, taking into account approaches for the layered display of policy information, policy templates, or policy icons.[53] This will depend on the circumstances of the processing and the mediums used to communicate information.

In contrast to the current framework with Directive 95/46 EC, the General Data Protection Regulation imposes stronger information obligations upon the controller, whereby the law differentiates between two cases:

- Personal data are collected from the data subject (Art. 13 GDPR)
- Personal data have not been obtained from the data subject (Art. 14 GDPR)

When personal data are collected from the data subject (Art. 13 GDPR)

The typical examples for such cases are either when the controller directly asks the data subject for consent or when he obtains the information from the data subject when concluding a contract to provide goods or a service. Generally, the solutions proposed by SPECIAL will rather be applicable for existing relations between controller and data subject. An established channel for communication allows further communication regarding information for transparency or additional consent for pursuing other purposes with the obtained data.

- Art. 13 paragraph 1 of the GDPR:

[53] See Art. 12 (7) GDPR. See also the results from the PrimeLife-project in Holtz, Zwingelberg, H.; Hansen, M.: '*Privacy Policy Icons*', a dedicated book chapter in: *'Privacy and Identity Management for Life*', pp 279-285, p. 279 et. seq.

In such a context, the controller is obliged to provide **at the time of data collection** the following information:

- The **controller's identity, contact details** and of the controller's representative (if there is one). The data provided must enable the data subject to contact the data controller and where necessary without media disruption, e.g. by providing an e-mail address. The **contact of the data protection officer** (if there is one)
- The **purposes of the processing and the associated legal basis**
  - This could under certain circumstances require several informative declarations of the controller when a number of different processing operations are based on different legal grounds or for several purposes. This is a central requirement closely related to the general principle of purpose limitation set forth in Art. 5 para.1 (b) GDPR.[54] Evidently, this demands that the controller must think about and define the purposes in writing before any personal data collection or processing and consider the appropriate legal basis for each of the purposes. The description of the legal basis must be in a form that the data subject can follow the line of argumentation, and at least for more complex legal grounds, it is insufficient to just cite the legal norm – usually a paragraph of Art. 6 GDPR. Instead, the controller has to substantiate how the norm covers the envisaged processing procedures.[55] This may cause problems for some big data applications where the purposes were not previously defined. Insofar, the GDPR's transparency requirements set limits to the extensive use of personal data in big data environments. Where the processing is based on consent, a new consent can be obtained.[56] Here, the planned SPECIAL specifications for communication by automated means between controllers and data subjects may provide a viable solution for data controllers.
    In the light of the steadily growing market for big data analysis, the legislator – more precisely the European Council – demanded a relaxation of the purpose limitation requirement. Due to the strict opposition of the European Parliament, this intent was mainly dropped and led to a compromise in favour of the parliament.[57] In Art. 6 para. 4 GDPR, it is allowed to process data for purposes compatible with the purpose the data has initially been collected for. However, this compromise comes for data controllers to the cost of strict transparency-requirements towards data subjects set forth in Art. 13 para. 3 GDPR. Also, each new purpose must be covered by an own legal basis, as opening the purpose limitation principle for compatible purposes was clearly not intended to undermine the protection of the pre-existing Directive 95/63/EC.[58]
- The **legitimate interests**, when they provide a basis for processing by the controller or a third party
  - This relates to the requirement that the legal basis must be understandable. Where processing is based on legitimate interests of the controller pursuant to Art. 6 para. 1 (f) GDPR, these interests must be clearly described, so data subjects can decide whether they want to exercise their right to object, Art. 21 GDPR.

[54] Schantz, P., 'Die Datenschutz-Grundverordnung – Beginn einer neuen Zeitrechnung im Datenschutzrecht' (translated: '*The General Data Protection Regulation – Start of a New Era*'), Neue Juristische Wochenschrift (NJW) 2016, p. 1844.

[55] Kühling, Buchner (ed.), '*Datenschutzgrundverordnung – Kommentar*' (translated: '*General Data Protection Regulation – Commentary*'), see there Prof. Dr. Bäcker about Art. 13 GDPR para. 26.

[56] See the clear exception in Art. 4 para. 1 GDPR.

[57] Albrecht, Jotzo, '*Das neue Datenschutzrecht der EU – Grundlagen / Gesetzgebungsverfahren / Synopse*', (translated: 'The New Data Protection Law of the EU – Basis /Legislative Process /Synopsis'), page 52.

[58] Kühling, Buchner (ed.), there Buchner, B. and Prof. Dr. Petri about Art. 6 GDPR para. GDPR, page 182; Albrecht, Jotzo, p. 52; Schantz, NJW 2016, p. 1844.

- The **recipients or categories of recipients** of the data

  Usually, the concrete recipients have to be named; only when this is very difficult for the controller, the mere categories can be sufficient. An example could under certain circumstances be a group or pool of advertisement partners. However, this possibility is usually the exception and such an approach should be well-justified by the controller. According to Art. 4 para. 9 GDPR, the term '*recipient*' does not only refer to third parties. This also covers data processors, departments, or subsidiaries of the data controller that must be named.[59] Where the data will be published, this fact must be stated, but it is not necessary to list potential recipients.

- **If data transmissions to third countries or international organisation is intended**, including **information about** the data protection level in said country **('existence or absence of adequacy decision by the European Commission')**, and additionally, **when no adequacy decision** exists, where the **information about the appropriate safeguards or Binding Corporate Rules** are available which provide a global code of practice based on EU data protection standards that allow the transfer of personal data.

  This is to enable understanding of the legal basis of planned cross-border data transmissions outside of the EU and allow risk estimation for the data subject.

- Art. 13 paragraph 2 of the GDPR:

Further information obligations for the controller defined in paragraph 2 intend to ensure fair and transparent processing and shall likewise be provided **at the time of data collection**:

- **Duration of data storage** or the criteria of the storage period determination
  - Here, it might be practical for the controller to determine this for specific categories of data, including the reason for the specific storage period. The mention of mere criteria is also usually the exception when the concrete determination of a storage period is not possible; such an approach needs to be well-justified by the controller.
- **Information about the data subject's rights** (access, rectification, erasure, restriction of processing and data portability)
  - Ideally, this information comes tailored to the circumstances of the concrete processing operation involved
- **Information about the right to withdraw consent at any time** if the processing is based on consent explaining its ex nunc effect, thus that previous processing is not affected by the withdrawal of consent.
- **Information about the right to lodge a complaint with a supervisory authority**
  - Ideally, already with contact information of the competent supervisory authority
- **Information about why the provision of the data is necessary**, e.g. data provision required by law or contract, or needed to conclude a contract. Furthermore, **whether the data subject is obliged to provide this data and the consequences of a failure to do so**
- **Information about the existence of automated decision-making, including profiling** and **meaningful information about the logic involved, its significance and envisaged consequences for the data subject**

  The goal here is that the data subject knows that he/she is being profiled, in which way, and why. '*Meaningful*' indicates that this information should be comprehensible for the average data subject/end user. This would mean that too vague and broad information

[59] Kühling, Buchner (ed.), there Prof. Dr. Bäcker about Art. 13 GDPR para. 30.

will not suffice. To this purpose, the involved logic and the algorithms and criteria used must be described.[60]

Finally,further information obligation is regulated in paragraph 3 of Article 13, which requires **information to be provided to the data subject when the controller intends to further process the personal data for another purpose** than the original one. This information must occur **prior to the further processing and together with relevant further information as mentioned above for paragraph 2**.

Here, it is advisable for the controller to check in advance what information needs to be given based on the new purpose(s), for example when any recipients of the data change or the like. Again, the information provided needs to be in a form that the data subject can derive a vision about the processing entities' identity, how the processing takes place and the related risks. This requirement raises specific challenges in the field of big data analytics[61] which are so far not finally settled in legal literature. Where data will be transferred to a third party who plans to use the data for a new purpose, the data controller initially obtaining the data must provide the information.[62]

- Exception of the above information obligations (Art. 13 para. 4 of the GDPR):
  - Only if the data subject already has all the information in the necessary granularity, this exception holds. Therefore, is not sufficient if the data subject has only a general oversight. Furthermore, the data subject must have the information in its own sphere, which means it is usually insufficient if the information is publicly somewhere in the internet or otherwise available for the data subject.

When personal data have not been obtained from the data subject (Art. 14 GDPR)

In cases where the personal information related to the data subject has been obtained from other sources, Article 14 demands even further information going beyond the obligations of Article 13 GDPR. Examples of further information to provide (besides the information as like in Art. 13) are:

- Information about the **categories of personal data concerned** (Art. 14 para. 1 (d) GDPR)
- **Information about the data source** and if applicable, whether it came from publicly accessible sources (Art. 14 para 2 GDPR)

  Informing about the source enables data subjects to contact the source and to e.g. object to further disclosure of personal data. Therefore, this constitutes an important prerequisite for the effective execution of data subject's rights, including the right to be forgotten in relation to the responsible controller. In cases where this might be difficult because e.g. the data stems from various sources, Recital 61 GDPR mentions that general information may suffice. However, for this exception, it must be taken into account that failure to name the sources deprives data subjects from their possibility to refer to the source and e.g. to object to further disclosure. Therefore, this exception must be applied with reluctance.[63] Rather, data controllers shall store the information about the source and where possible, the initial purposes pursued together with the relevant information. As this is one of the features of the specifications SPECIAL plans to provide, the foreseen solution has one of its roots and legal necessity in this norm. Once the policy information

[60] Kühling, Buchner (ed.), Prof. Dr. Bäcker about Art. 13 GDPR para. 45.

[61] Paal, B. P.; Pauly, D. A., '*Datenschutz-Grundverordnung*' Art. 13 GDPR para. 37.

[62] Kühling, Buchner (ed.), Prof. Dr. Bäcker about Art. 13 GDPR para. 70.

[63] Kühling, Buchner (ed.), Prof. Dr. Bäcker about Art. 14 GDPR para. 20.

is stored accordingly, the data subjects can be informed with sufficient detail. So in such cases, it seems advisable to describe exemplary sources and whether these are public or non-public, respectively whether the majority of data stems either form public or non-public sources.

Another central information can be taken from Art. 14 para. 2 (f) GDPR: Personal data is not open to unlimited use or processing when it had been public before, not even if it was published by the data subject herself. While in this case often Art. 6 para. 1 (f) GDPR will provide and applicable legal ground, this does not directly affect the information duties of the collecting controller according to Art. 14 GDPR, unless an exception of Art. 14 para. 5 GDPR applies (see below).

For big data in general and for some aspects of the SPECIAL use cases in particular, it is crucial to inform data subjects about the means of obtaining the data. This applies in particular where this is not obvious from the knowledge of the source and the data. This may be the case when the data controller not only collects personal information which has been self-published by the data subject, e.g. on a website or social networks. Rather, this applies as well when information is analysed and profiled by the controller to gain additional information about the data subject.[64]

Article 14 para. 3 (a) manifests **specific timing when the information must be given:**

- Usually **within a reasonable period** after obtaining the data, but **at the latest within one month**
- When intention of the data collection is the communication with the data subject then **at the time of the first communication**
- When a disclosure to another recipient is intended, then **at the time of first disclosure**

When further processing of personal data for another purpose is intended, new information related to that new processing must be given **prior to its execution** (Art. 14 para. 4).

- ❖ <u>Exceptions of the above information obligations (Art. 14 para. 5 GDPR):</u>
  - ➢ If the data subject already has all the information
  - ➢ The provision of the information is impossible or would involve a disproportionate effort
    - ➢ In particular, a disproportionate effort can be given for processing for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes. These categories of examples have in common that massive amounts of data are involved and that a commonly accepted and privileged purpose is pursued. In the named cases, the legislator anticipated a weighing of interests, which means that in all cases, a detailed analysis of conflicting interests is required. This includes the data subject's interest in getting the information on one side and the burden for the controller to inform the data subject on the other side.[65] Where e.g. data is obtained from public sources, and no additional danger is added by the type of processing, e.g. by profiling or linking with other

[64] Kühling, Buchner (ed.), Prof. Dr. Bäcker about Art. 14 GDPR para. 21.

[65] Albrecht, Jotzo, p. 84; Kühling, Buchner (ed.), Prof. Dr. Bäcker about Art. 14 GDPR para. 55. With focus on genetic big data see Pormeister, K., '*The GDPR and Big Data: leading the way for Big Genetic Data?*', proceedings of the Annual Privacy Forum, Vienna 2017, section 3.2.

information, the controller's interest tends to prevail. But were the type of data, or the processing itself poses a risk to the data subject, the exception will not be able to excuse the controller from its duty to inform the affected persons. Hence, transparency requirements pose a major challenge for big data. Useful and comprehensible approaches to communicate the relevant information to the data subjects and, where necessary, to provide a way to obtain consent lies in the central interest of controllers. Another example case is when the information would render impossible or seriously impair the achievement of the processing objectives. Whenever this exception takes effect, the controller has alternate obligations to take appropriate measures for the protection of the data subject's rights and freedoms and legitimate interests. This can be achieved e.g. by additional security measures, the deployment of PETs, and by making the information about the processing publicly available.

- When obtaining or disclosure is expressly laid down in Union or Member State law and which provides appropriate measures to protect the data subject's legitimate interests
- When the controller has contradicting confidentiality obligations of professional secrecy based on Union or Member State law.

2.2.7 Usage of privacy-enhancing technologies

The intention of the European Union to initiate the data protection framework - beyond harmonization of the rules across Europe – was to give individuals more protection and control over their personal data. In doing so, the GDPR provides for an improved level of protection for individuals across the whole Union.

With the adoption of the General Data Protection Regulation, the principles of data protection by design and by default have found its way into this regulatory instrument. The GDPR provides for specific rules for data security (Art. 32 GDPR), plus the general demand to protect the personal information of individuals by means of technical and organisational measures (Art. 24, 25 GDPR).

The obligation to implement appropriate technical and organisational measures for protection directly addresses the controller of the processing, but not the providers of processing systems, such as hardware and software/app manufacturers.

Still, according to Article 25 para. 1 GDPR (Data protection by design and by default), the controller must consider these technical and organisational measures already when determining '*the means for processing and at the time of the processing itself*'. This wording strongly suggests that in future, the controller is obliged to choose only such processing systems which can comply with the above explained data protection principles. This assumption is supported by comments from the legislators in Recital 78, which says that **'***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.*' Furthermore, Recital 87 states that data protection by design and by default should be part of public tenders. When it comes to data protection by default, this is a big part of the opt-in vs. the opt-out approach, whereas the opt-in to data-based services is promoted strongly in the GDPR. Other, non-conclusive examples for technologies supporting privacy by design and by default are anonymization, pseudonymization, sticky policies, automated procedures for obtaining informed consent in user-friendly manner and the provision of functionalities to manage own personal information, whereas e.g. the first two are explicitly mentioned as examples in the GDPR.

It requires a systematic approach to determine technical and organisational measures. A good example for such an approach is the Standard Data Protection Model developed by the national data

supervisory authorities in Germany.[66] This model serves as a tool to translate sometimes rather abstract legal requirements into concrete functional and organisational requirements. It is based on six data protection goals, whereby the already well-known classical IT security goals confidentiality, integrity and availability have been integrated. To take the fundamental rights perspective more into account, three additional protection goals complement these, which are unlinkability (+ data minimization), intervenability and transparency. This approach will be used later on during the SPECIAL project to translate law into technology by the application of the protection goals to data, systems and processes, alongside with a determination of required level of protection for the personal information involved.

[66] Cf. Standard Data Protection Model: https://www.datenschutzzentrum.de/sdm/ .

2.3 Upcoming ePrivacy Regulation

In this chapter, the draft of the ePrivacy Regulation (in the following: draft ePR), as proposed by the European Commission in January 2017, will be introduced. The ePrivacy Regulation is also meant to be applicable by 25 May 2018, repealing the current ePrivacy Directive.[67] This new regulation is meant to complement the GDPR in the field of electronic communications, whereby only as far as personal data is concerned, it will be applicable instead of the GDPR (lex specialis).

However, the legislative process of the draft ePR is still ongoing. At the time of writing this deliverable, the draft text of this regulation is under review by the Council and the Parliament while it is at the time being not foreseeable whether changes will be proposed. The draft text has already been heavily criticised for providing a much weaker level of protection compared to the GDPR as well as for having an extensive yet unclear scope, unclear wording, and rules partially not matching the reality of the industry landscape. So it must be assumed that the draft ePR text is still in flux, making for the time being concluding statements regarding the legal requirements in the context of electronic communications difficult. Consequently, this deliverable will just provide a short overview over the core preconditions as laid down current draft ePR. While doing so, it will highlight criticism and uncertainties pointed out by relevant stakeholders having influence on the legislative process. While even data-driven IT businesses and their representatives have expressed dissatisfaction with the current draft[68], the analysis of this chapter will refer mostly to three main sources, which are:

- Opinion 6/2017 of the European Data Protection Supervisor (EDPS) Giovanni Buttarelli, titled '*EDPS Opinion on the Proposal for a Regulation on Privacy and Electronic Communications (ePrivacy Regulation)*', published 24th of April 2017.
- Article 29 Working Party, '*Opinion 01/2017 on the Proposed Regulation for the ePrivacy Regulation (2002/58/EC)*' adopted on 4 April 2017, WP 247.
- A study by Dr. F. Zuiderveen Borgesius et al. from the Institute for Information Law (IviR), University of Amsterdam, titled '*An Assessment of the Commission's Proposal on Privacy and Electronic Communications*'. This study was requested by the European Parliament's LIBE Committee and commissioned by the European Parliament's Directorate General for internal Policies, Policy Department C: Citizen's Rights and Constitutional Affairs, published June 1st 2017. This study will hereinafter be abbreviated as **IPOL study**.

These three statements provide very in-depth legal analysis of the draft ePR with a strong focus on the fundamental rights protection of individuals whose personal data might be collected and processed in the course of electronic communications. Therefore, crucial criticism points detailed therein will be highlighted.

[67] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).

[68] Cf. for example the statement of the German IT business association BITKOM, which can be found under: https://www.bitkom.org/noindex/Publikationen/2017/Positionspapiere/FirstSpirit-1493795654847201704 27-E-Privacy-Stellungnahme-FIN.pdf. Furthermore, see the article by Ulessi, C. 'EU: Draft ePrivacy Regulation set to pose "considerable burdens for companies"', published January 12th 2017 on Dataguidance.com which gives an overview of business-sided reactions to the ePR draft.

2.3.1 Application scope

The application scope of the draft ePR is regulated in its Article 2 (material scope) and Article 3 (territorial scope). In general, the draft ePR is focused at electronic communications data, which includes meta- & content data. In comparison to the former ePrivacy Directive which it repeals, the scope has been extended significantly, now including Over-The-Top (OTT) providers and services. OTT communication services are often differentiated between OTT1 (communication) services and OTT2 (content) services. The BEREC[69] provided a rough definition of the different OTT services, which are:

- OTT-0 which are Electronic Communications Services (ECS)
- OTT-1 which are not ECS, yet potentially compete with them
- OTT-2 which are any other information society services[70]

However, a clear distinction between those is often not possible since many services like social media, webmail, and messaging apps often offer communication platforms as well as integrated, connected services. Services like music streaming or video-on-demand often profile usage behaviour beside the core service of media provision. In terms of terminology, it must also be noted that the draft ePR in many cases does not provide its own terminology but rather refers to definitions given in another new legal instrument still being in the midst of a legislative process. This is the draft proposal for a Directive establishing a European Electronic Communications Code (hereinafter: **draft EECC**).[71] Moreover, references are being made to some terminology in the GDPR and to the Directive 2008/63/EC on competition in the markets with respect to telecommunication terminal equipment.[72] As a result, inconsistencies and uncertainties with regard to the factual scope are caused. In the following, some examples of these inconsistencies and uncertainties will be presented, sometimes highlighting those aspects which might play a role for the actual use cases of the SPECIAL project.

(a) Material scope

The material scope is regulated in Art. 2 draft ePR, which states (bold highlights added):

> '*1. This Regulation applies to the **processing of electronic communications data** carried out in connection with the **provision and the use of electronic communications services** and to **information related to the terminal equipment of end-users**.*
>
> *2. This Regulation does not apply to:*
>
> *(a) activities which fall outside the scope of Union law;*
>
> *(b) activities of the Member States which fall within the scope of Chapter 2 of Title V of the Treaty on European Union;*
>
> *(c) electronic communications services which are not publicly available;*
>
> *(d) activities of competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security;*'

[69] Body of European Regulators for Electronic Communications.

[70] See the BEREC's '*Report on OTT services*', BoR (16) 35 of January 2016, page 6.

[71] European Commission, Corrigendum: '*Proposal for a Directive of the European Parliament and of the Council establishing the European Electronic Communications Code (Recast)*', COM(2016) 590 final/2, Brussels, 12.10.2016.

[72] Commission Directive 2008/63/EC of 20 June 2008 on competition in the markets in telecommunications terminal equipment (OJ L 162, 21.6.2008, p. 20–26).

For the determination of applicability, a clear understanding of the terminology is necessary. Of relevance here are with reference to the text of Article2, the following terms:

- Electronic communications data
- Electronic communications service
- Terminal equipment
- Users and end-users

Electronic communications data

According to Article 4 para. 3 (a) draft ePR, the term '*electronic communications data'* is to be understood as being

> '*electronic communications content and electronic communications metadata*'.

Content is to be understood as

> '*the content exchanged by means of electronic communications services, such as text, voice, videos, images, and sound*' (Art. 2 para. 3 (b)).

Metadata is defined as follows:

> '*electronic communications metadata' means data* ***processed in an electronic communications network*** *for the* ***purposes of transmitting, distributing or exchanging electronic communications content****; including* ***data used to trace and identify the source and destination of a communication, data on the location of the device*** *generated in the context of providing electronic communications services, and the* ***date, time, duration and the type of communication****;*'

The term '*electronic communications network*' is not directly defined in the draft ePR. Rather, Art. 4 para. 2 (b) of the draft ePR refers to definitions given in the draft EECC.

There, this term is defined in Article 2 (1) as follows:

> '*(1) 'electronic communications network' means* ***transmission systems****, whether or not based on a permanent infrastructure or centralised administration capacity, and, where applicable, switching or routing equipment and other resources, including network elements which are not active, which permit the conveyance of signals by wire, radio, optical or other electromagnetic means, including satellite networks, fixed (circuit- and packet-switched, including Internet) and mobile terrestrial networks, electricity cable systems, to the extent that they are used for the purpose of transmitting signals, networks used for radio and television broadcasting, and cable television networks, irrespective of the type of information conveyed;*'

The use of the draft EECC's definitions of metadata with strong connection to the term '*network*' has been criticized by the Article 29 Working Party as eventually being too narrow as it may cover only the provision of services in the lower layer of the network, excluding data generated outside of a network, such as during the provision of an OTT service.[73] The same criticism has been made by the IPOL study[74] and by the EDPS, who highlighted that a broad scope of the term 'metadata' is needed to ensure a high level of protection for individuals. He emphasized that metadata information, such as from mobile location data, can be used to derive sensitive information about a person's life, such

[73] Article 29 Working Party, WP 247, page 16.

[74] Cf. IPOL study, page 48.

as '*political leanings and associations, medical issues, sexual orientation or habits of religious worship can be discovered through mobile phone traffic data*'.[75] This viewpoint is backed by a decision of the CJEU who in two joined cases that this data '*is no less sensitive, having regard to the right to privacy, than the actual content of communications.*'[76]

Electronic communications service

Article 4 of the draft ePR stipulates definitions, for the terms 'electronic communications service' and 'end-user', para. 1 (b) refers directly to definitions given in the draft EECC. Article 2 (4) draft EECC defines this term as follows:

> '*(4) 'electronic communications service' means a* ***service normally provided for remuneration via electronic communications networks****, which encompasses* ***'internet access service'*** *as defined in Article 2(2) of Regulation (EU) 2015/2120; and/or* ***'interpersonal communications service'****; and/or* ***services consisting wholly or mainly in the conveyance of signals*** *such as transmission services used for the provision of machine-to-machine services and for broadcasting,* ***but excludes services providing, or exercising editorial control over, content transmitted using electronic communications networks and services****;*'

From this definition, it is not entirely clear whether services without paying remuneration are included in this definition of electronic communications service. The wording 'normally provided for remuneration' suggests that other provision models (e. g. by 'paying with your data,' and acceptance of advertisement) are possible, yet this is not very explicit in this text.

'Interpersonal communications service' is defined in Art. 2 (5) of the draft EECC as follows:

> '*(5) 'interpersonal communications service' means a service normally provided for remuneration that* ***enables direct interpersonal and interactive exchange of information via electronic communications networks between a finite number of persons****, whereby the persons initiating or participating in the communication determine its recipient(s); it does not include services which enable interpersonal and interactive communication merely as a minor ancillary feature that is intrinsically linked to another service;*'

However, this definition is complemented by an amendment in Article 4 para. 2 draft ePR, which explicitly includes ancillary features. From the draft EECC definition, it becomes clear that so-called OTT-1 services like social media, internet messengers and webmail would be included; however, the information exchange is limited to being between finite numbers of persons. This would mean that services directed at a potentially infinite number of persons, like websites, broadcasting & video on demand sites, open content of social networks (outside closed groups or restricted 'friends-only' access), or blogging sites are not considered being '*interpersonal communications services*'

Recital 13 of the draft ePR says that the regulation '*should not apply to closed groups of end-users such as corporate networks, access to which is limited to members of the corporation.*' The Article 29 Working Party has pointed out already in their 2008 opinion on the ePrivacy Directive that sometimes the distinction between a private or public network is difficult to make.[77]

[75] EDPS Opinion 6/2017, page 28.

[76] CJEU judgement of 21 December 2016 in joined cases C-203/15 (Tele2 Sverige AB) and C-698/15 (Watson), para. 99 f.

[77] Article 29 Working Party, WP 150, page 4.

Terminal equipment

Article 4 para. 1 (c) refers for the definition of '*terminal equipment*' to point (1) of Article 1 of Commission Directive 2008/63/EC.[78] This directive provides the following definition:

> '*1. 'terminal equipment' means:*
>
> *(a) equipment* ***directly or indirectly connected to the interface of a public telecommunications network to send, process or receive information****; in either case (direct or indirect), the connection may be made by wire, optical fibre or electromagnetically; a connection is indirect if equipment is placed between the terminal and the interface of the network;*
>
> *(b) satellite earth station equipment;*'

From this definition, any device being able to connect to a public telecommunications network could be terminal equipment, be it an internet router, PC, laptop, tablet, internet-enabled games console or IoT device, or a smartphone.

User and end-user

Since the draft ePR is not specifically aimed at the regulation of personal data, rather of electronic communications, it does not focus on the same concepts as the GDPR in relation to natural persons as data subject, or controllers and processors. Rather, it uses terminology like '*user*' and '*end-user*'.

For the term '*end-user*', the draft ePR refers to the definitions in the draft EECC proposal. Article 2 (13) draft EECC provides a definition for a '*user*':

> '*(13) 'user' means a* ***legal entity or natural person*** *using or requesting a publicly available electronic communications service;*'

In contrast, an '*end-user*' is according to Art. 2 (14) draft EECC:

> '*(14) 'end-user' means a* ***user not providing public communications networks or publicly available electronic communications services****.*'

In these two definitions, no differentiation is being made between a natural person and a legal entity, for example a company or other organisation. End-users will in most cases be natural persons only, while companies could be both. An example for illustration would be the company subscribing to electronic communications services which might decide to provide (as user) these services to its employees (who would then be the end-users). The inclusion of legal persons in the definition of 'end-user' has been criticized by the EDPS as being problematic. The argument of the EDPS is that only an unambiguous focus on the individual as data subject when using electronic communications services can ensure a good protection of this individual's fundamental rights. Thereby, he used specifically the company-employee example to emphasize the need of protection.[79] Furthermore, the IPOL study points out that a machine does not fall under these definitions.[80]

[78] Directive 2008/63/EC of 20 June 2008 on competition in the markets in telecommunications terminal equipment.

[79] EDPS Opinion 6/2017, page 12 f.

[80] IPOL study, page 42.

As it becomes clear from the above elaborations, some of these definitions have some shortcomings either in scope or clarity. This is also amplified by the fact that other provisions in the draft ePR derive from these definitions or assumptions of scope. So for example, Recital 8 of the draft ePR provides some examples of electronic communications services which seem much broader than the actual application scope of Article 2, stating that:

> '*This Regulation should apply to providers of* ***electronic communications services****, to providers of* ***publicly available directories****, and to* ***software providers permitting electronic communications, including the retrieval and presentation of information on the internet****. This Regulation should also apply to* ***natural and legal persons who use electronic communications services to send direct marketing commercial communications or collect information related to or stored in end-users' terminal equipment.****'*

Furthermore, Article 3 draft ePR reveals more discrepancies. Article 2 para. 1 has its focus on '*the* ***processing*** *of electronic communications* ***data***' for the application scope, while the above elaborations have shown that it is unclear whether services without remuneration are included. In contrast, Article 3 para. 1 (a) refers to '*the* ***provision*** *of electronic communications to end-users in the Union,* ***irrespective of whether a payment of the end-user is required****.*' This is a notable inconsistency in wording. In conclusion, the current draft implies much legal uncertainty already regarding its material application scope. Some examples can be given for services within the draft ePR material application scope:

- Telephone calls and SMS
- Voice over IP
- Internet messenger services
  - This is relatively clear for the content, yet not entirely clear for metadata generated by such services.
- Web browsing behaviour (URL's)
  - Recital 2 of the draft ePR names web browsing behaviour as an example to fall under the scope. However, this is not explicit from the text of the draft ePR itself.
- Included are also interpersonal communications services which are ancillary to other services

Unclear with regard to applicability of the draft ePR are for example:

- WiFi hotspots
  - Recital 13 draft ePR mentions only some specific examples to fall within the application scope: '*"hotspots" situated at different places within a city, department stores, shopping malls and hospitals*'. Not included in these examples are '*Wi-Fi services in hotels, restaurants, coffee shops, shops, trains, airports and networks offered by universities to their students, as well as corporate Wi-Fi access offered to visitors and guests, and hotspots created by public administrations.*'[81]
- Machine-to-machine communication
  - This may concern especially connected devices in the context of the Internet of Things (IoT), sensors, or smart TV's.
- Services which process data by any other equipment outside of a '*communications network*', such as by '*associated facilities*' in the sense of the EECC.

[81] EDPS Opinion 6/2017, page 25.

- Communication which is not stored on end-users terminal equipment, but in a cloud (e.g. in-platform messages in social media (e.g. Facebook, Twitter, Internet mail), or in-app messages in games.[82]

Especially the IPOL study highlighted that the EU lawmakers should pay very close attention to the legislative process of the draft EECC since any changes of the definitions could have severe impact on the draft ePR.[83] The IPOL study, the Article 29 Working Party, and the EDPS made several improvement suggestions for the wording of the application scope and all of them strongly suggested to eliminate the reliance on the definitions of the draft EECC by providing own definitions directly in the draft ePR. As changes are being made during the legislative process of the draft ePR, these will be closely watched in the context of the legal research work for SPECIAL and for the legal analysis of the project's use cases.

(b) Territorial scope (Art. 3 draft ePR)

Article 3 draft-ePR manifests the territorial scope of the regulation, stating that:

> '*1. This Regulation applies to:*
>
> *(a) the provision of electronic communications services to end-users in the Union, irrespective of whether a payment of the end-user is required;*
>
> *(b) the use of such services;*
>
> *(c) the protection of information related to the terminal equipment of end-users located in the Union.*'

Article 3 assumes applicability once electronic communications services are provided to end-users who are located within the European Union. In addition, Recital 9 of the draft ePR further clarifies that this applies '*regardless of whether or not the **processing** takes place in the Union*' and to '*electronic communications data processed in connection with the **provision of electronic communications services from outside the Union to end-users in the Union**.*'

Nonetheless, some uncertainties remain, as the above described inconsistency in wording compared to Article 2 shows. Moreover, the IPOL study states that the territorial scope would be unclear with regard to parties located outside the EU which violate either Article 15 (on phone books and public directories) or Article 16 (on unsolicited communications and spam). Therein, the study called for further clarification as well.[84]

According to the paragraphs 2-5 of Article 3, the provider of an electronic communications service who is not established in the EU is obliged to designate in writing a representative established in a Member State of the Union where end-users reside. The representative has to function as a contact and information source in particular for to supervisory authorities and end-users.

[82] This was also mentioned and criticized by the European Data Protection supervisor as leaving significant gaps in individual's protection of their communication, see EDPS Opinion 6/2017, page 13.

[83] IPOL study, page 33.

[84] Ibidem, page 30.

2.3.2 Basic principles

Recital 5 of the draft ePR states that the '*Regulation therefore does not lower the protection enjoyed by natural persons under the'* [GDPR]. However, the articles of the draft ePR do not say much about the concrete relationship to the GDPR in general. Some – but not all - key data protection principles from the GDPR appear in the draft ePR as well, for example, confidentiality, transparency, and accountability aspects.

(a) Confidentiality of electronic communications data

One of the core principles which plays a role in the draft ePR is the communication secrecy manifested in Article 5 draft-ePR:

> '*Electronic communications data shall be confidential. Any interference with electronic communications data, such as by listening, tapping, storing, monitoring, scanning or other kinds of interception, surveillance or processing of electronic communications data, by persons other than the end-users,* ***shall be prohibited, except when permitted by this Regulation.***'

Similar as in the GDPR, there is a principle of prohibition with permission reservation, making a legal ground for the interference with electronic communications data mandatory. In this context, the question is what counts as '*interference*' in the sense of Article 5. Recital 15 of the draft ePR gives some examples from the EU lawmakers what they have seen in principle as a violation of the communication secrecy:

> '*The prohibition of interception of communications data should apply during their conveyance, i.e. until receipt of the content of the electronic communication by the intended addressee. Interception of electronic communications data may occur, for example, when someone other than the communicating parties,* ***listens to calls, reads, scans or stores the content of electronic communications, or the associated metadata for purposes other than the exchange of communications.*** *Interception also occurs when third parties* ***monitor websites visited, timing of the visits, interaction with others, etc., without the consent of the end-user concerned.*** *As technology evolves, the technical ways to engage in interception have also increased. Such ways may range from the* ***installation of equipment that gathers data from terminal equipment over targeted areas****, such as the so-called IMSI (International Mobile Subscriber Identity) catchers, to* ***programs and techniques that, for example, surreptitiously monitor browsing habits for the purpose of creating end-user profiles.*** *Other examples of interception include* ***capturing payload data or content data from unencrypted wireless networks and routers, including browsing habits without the end-users' consent****.'*

The list of these examples is not conclusive and is also much broader than the actual Article 5. This raises questions whether the following cases pose communication secrecy violation as well:

- Machine-to-machine communication
  - Examples could be metering devices and sensors connecting to a data centre.
- Injection of advertisement, identifiers or other content
  - Examples could also be tracking cookies

As for data being in storage instead of being in transit, the first sentence of Recital 15 seems to suggest that data would be protected by the draft ePR only during conveyance, something the Article

29 Working Party expressed worry about.[85] However, Article 5 itself refers to '*any interference*' with electronic communications data, making it more clear that the application scope extends also over data that is stored. The European Data Protection Supervisor welcomed the extension of the confidentiality obligations to OTT providers. He highlighted that the '*right to the confidentiality of communications is a fundamental right protected under Article 7 of the Charter of Fundamental Rights of the European Union.*'[86] However, he criticised that by differentiating between metadata, content data, data emitted by terminal equipment also in the later legal permissions to process these, different levels of confidentiality are established. This may lead to a risk of unintended gaps in protection of data subjects.[87] Another point of criticism is that application scope should make it more clear that all collection and processing '*of electronic communications data (…) should unambiguously come under the scope of the ePrivacy Regulation, irrespective of which entity processes such data.*'[88] This is something that appears unclear to many when taking into account activities of data processors getting involved on the behalf of data controllers in the sense of the GDPR.[89] The IPOL study focuses on a more consistent protection of the communication secrecy as well, pointing out the importance of a better definition of metadata, of a more stringent necessity principle, and of a creation of a better power balance between service providers and end-user to mitigate take-it-or-leave-it situations. Moreover, the right to communication confidentiality should be complemented by '*the right to impart and receive information, and related rights.*' Furthermore, the value of encryption to communication secrecy should be acknowledged by the EU lawmakers.[90]

(b) Information and options for privacy settings to be provided

Article 10 draft ePR regulates the information and options which should be provided by software permitting electronic communications. With the obligations stipulated in Article 10, the EU lawmakers wanted to counter the problem of end-users being *'[…] increasingly requested to provide consent […]'*[91] Therefore, information and options provided already in the software being used is meant to lift this burden. Article 10 draft ePR stipulates:

> '*1.* ***Software*** *placed on the market* ***permitting electronic communications****, including the retrieval and presentation of information on the internet,* ***shall offer the option to prevent third parties from storing information on the terminal equipment of an end-user or processing information already stored on that equipment****.*
>
> *2.* ***Upon installation****, the software shall* ***inform the end-user about the privacy settings options*** *and, to continue with the installation,* ***require the end-user to consent to a setting****.*'

Therefore, the following functionalities have to be provided to an end-user:

- Possibility to prevent third parties from storing information on the terminal equipment
  - This can most likely concern the storage of cookies on a device
- Possibility to prevent third parties from processing information already stored on the terminal equipment
  - This can most likely concern device fingerprinting or other identifying processing

Additionally, already upon the installation of the software, the end-user must receive:

[85] Article 29 Working Party, WP 247, page 26.

[86] EDPS Opinion 6/2017, page 6.

[87] Ibidem, page 3.

[88] Ibidem, page 16.

[89] Cf. Engeler, M., Felber, W., '*Entwurf der ePrivacy-VO aus Perspektive der aufsichtsbehördlichen Praxis*' (roughly translated: The draft of the ePR from the perspective of DPA practice), ZD 6/2017, p. 253.

[90] IPOL study, page 9 f. + 12.

[91] See Recital 22 draft ePR for the example of overloading end-users with consent requests in cookie-banners.

- Information which privacy setting options the software provides
- A request to consent to a setting before the continuation of the installation
  - Notably, it is not required to have a specific setting such as privacy by default setting. Nonetheless, the end-user must get the information that such a setting is possible.

As already indicated above, the EU lawmakers gave some explanations in Recital 22 draft ePR why they have put emphasis on the privacy settings information:

> '*end-users are overloaded with requests to provide consent. The use of technical means to provide consent, for example, through transparent and user-friendly settings, may address this problem. Therefore, this Regulation should provide for the* ***possibility to express consent by using the appropriate settings of a browser or other application****. The choices made by end-users when establishing its* ***general privacy settings of a browser or other application should be binding on, and enforceable against, any third parties****.*'

Therein, the requirements of Article 10 are a drawback on the request of privacy by default, still open up possibilities to offer privacy-friendly settings and functionalities, such as Do Not Track (DNT) or layered approaches for differentiated consent requests tailored to the specific usage of the software. Specifically the Article 29 Working Party suggested making the DNT standard mandatory.[92] The general challenge for the above mentioned information and option provision obligations may lie in the realization of these requirements depending on context and device (e.g. stationary or mobile). The EDPS highlighted that a '*simple choice*' should be possible while still, '*consent must meet the requirements for consent as required under Article 4(12) GDPR, including not only consent being 'freely given', but also 'specific' and 'informed'.'*[93] The IPOL study reflected on this need for practicability and user-friendliness in one easily accessible interface, suggesting that eventually, further research and more legislation might be needed for compliance achievement.[94]

(c) Other information obligations regarding detected security risks and enabling end-user control

Article 17 draft ePR foresees that providers must inform end-users of particular risks that may compromise the security of networks and electronic communications services. If measures against these risks lie outside of the scope of the provider, the end-user should be informed about any possible remedies, including an indication of the likely costs involved.

Regarding the facilitation of end-user control over terminal equipment, primarily the Articles 12-14 draft ePR oblige electronic communications service providers to provide specified control features to end-users. Examples are by simple means and free of charge, preventing connected line identification in publicly available number-based interpersonal communications services, or the possibility to reject incoming calls.

[92] Article 29 Working Party, WP 247, page 4.

[93] EDPS Opinion 6/2017, page 19.

[94] IPOL study, page 84.

2.3.3 Legal ground and consent

The draft ePR provides for legal grounds which make the processing of electronic communications data permissible, such as consent or law. However, the draft ePR primarily differs between different cases in the context of electronic communication , for which permissions are regulated. These are:

- Permissions addressing the **processing of electronic communications data** (Article 6)
  - This includes content and metadata, inclusive restrictions and requirements for the storage or erasure of both (Article 7).
- Permissions addressing **information stored in or related to end-users' terminal equipment** (Article 8)
  - This includes
    - using processing and storage capabilities of the terminal equipment
    - or information collection from the terminal equipment
- Permissions addressing **publicly available directories** (Article 15)
- Permissions addressing **unsolicited communications for direct marketing** (Article 16)

(a) Permissions addressing the processing of electronic communications data (Article 6)

The legal permissions in Article 6 provide for a quite broad and rather unstructured accumulation of preconditions and cases for which electronic communications data may be processed. Paragraph 1 draft ePR states:

> '*1. Providers of electronic communications networks and services may process **electronic communications data** if:*
>
> *(a) it is **necessary to achieve the transmission of the communication, for the duration necessary** for that purpose; or*
>
> *(b) it is **necessary to maintain or restore the security** of electronic communications networks and services, or **detect technical faults and/or errors in the transmission** of electronic communications, **for the duration necessary** for that purpose.*'

Hereby, the core permission is the provision of the electronic communication service itself, applying for both content and metadata. Moreover, the security of the electronic communications can be a permissible purpose for processing. Both permission aspects have as additional preconditions the general necessity principle and a limitation regarding the necessary duration. However, in individual cases, it might eventually be difficult to determine which exact duration is really necessary to fulfil one of the above purposes.

Furthermore, it is not clear whether the security purpose can be understood in the sense of giving a legal ground for data collection and processing to combat spam and bot traffic. So it remains uncertain in which cases electronic communications network providers may be allowed to monitor, filter, or block network traffic.[95]

[95] Engeler, M., Felber, W., '*Entwurf der ePrivacy-VO aus Perspektive der aufsichtsbehördlichen Praxis*' (translated: The draft of the ePR from the perspective of DPA practice), ZD 6/2017, p. 254.

Paragraph 2 (a) and (b) of Article 6 focus on additional permissions for the processing of **metadata**:

> '*2. Providers of electronic communications services may process electronic communications* ***metadata*** *if:*
>
> *(a) it is* ***necessary to meet mandatory quality of service requirements*** *pursuant to [Directive establishing the European Electronic Communications Code] or Regulation (EU) 2015/2120 […]* ***for the duration necessary*** *for that purpose; or*
>
> *(b) it is* ***necessary for billing, calculating interconnection payments, detecting or stopping fraudulent, or abusive use of, or subscription to, electronic communications services****; or*
>
> *(c) […]****.***'

So based on those above preconditions, processing metadata is allowed for the following purposes:

- Ensuring the quality of the communication service provision
- Billing
- Calculation of interconnection payments
- Detection of fraudulent or abusive
  - use of electronic communications services or
  - subscription to electronic communications services

Beyond these purposes explicitly specified in the draft ePR, Article 6 para. 2 lit. (c) additionally mentions consent as a possibility to make the processing of metadata permissible, stating:

> '*2. Providers of electronic communications services may process electronic communications* ***metadata*** *if:*
>
> *(a) […]*
>
> *(b) […]*
>
> *(c) the* ***end-user*** *concerned has given his or her* ***consent to the processing of*** *his or her communications* ***metadata*** *for* ***one or more specified purposes****,* ***including*** *for the* ***provision of specific services*** *to such end-users,* ***provided that the purpose*** *or purposes concerned* ***could not be fulfilled by processing information that is made anonymous.***'

Necessary for valid consent is in this context that it is given

- by the **end-user** concerned
- for **one or specified purposes**
  - which may include the provision of specific services and
- that these **purposes could not be fulfilled with anonymous data**.

Therefore, an electronic communications provider is obliged to check first (prior to processing commencement) whether the intended purposes cannot be fulfilled with anonymous information (e.g. in cases of location-based data, anonymized geo-information for rough '*heat maps*').

Additionally, Article 9 para. 1 of the draft-ePR explicitly requires that the preconditions of valid consent in the GDPR must be complied with as well. According to the GDPR, this means that consent must be:

- freely given, specific, informed and unambiguous (for one or more specific purposes)
- possible to withdraw at any time
- a statement or clear affirmative action of data subject expressing agreement.[96]

Furthermore, Article 9 para. 3 draft ePR demands that end-users who have consented to such processing of metadata must receive a **reminder of their withdrawal right at a periodic interval of every 6 months**, as long as the processing continues.

For processing the **content** of electronic communications, the draft ePR foresees several additional cases based on consent. Article 6 para. 3 specifies:

> '*3. Providers of the electronic communications services may process electronic communications* ***content*** *only:*
>
> *(a) for the* ***sole purpose of the provision of a specific service*** *to an end-user,* ***if the end-user or end-users*** *concerned have given their* ***consent*** *to the processing of his or her electronic communications content* ***and*** *the* ***provision of that service cannot be fulfilled without the processing of such content****; or*
>
> *(b)* ***if all end-users concerned have given their consent*** *to the processing of their electronic communications content* ***for one or more specified purposes that cannot be fulfilled by processing information that is made anonymous, and the provider has consulted the supervisory authority****. Points (2) and (3) of Article 36 of Regulation (EU) 2016/679 shall apply to the consultation of the supervisory authority.*'

So for the processing of content, this means that valid consent requires:

- the **end-user or end-users** concerned have given their consent,
- the purpose is the **provision of a specific service** to an end-user and
- the provision of that **service cannot be fulfilled without the content data**.

Alternatively, consent for processing content is possible if:

- **all end-users** concerned have given consent
- for **one or more specified purposes** and
- that these **purposes could not be fulfilled with anonymous data** and
- the provider has **consulted the supervisory authority**.

Moreover, the above mentioned preconditions of the GDPR apply as well (Article 9 para. 1 draft ePR).

Furthermore, also those end-users who have consented to processing of their electronic communications content must get a **reminder of their withdrawal right at a periodic interval of every 6 months**, for the whole duration of the processing (Article 9 para. 3 draft ePR).

[96] For further details, see above chapter 2.2.5.

(b) Permissions addressing information stored in or related to end-users' terminal equipment (Art. 8)

Article 8 (1) draft-ePR differentiates between the

- use of processing and storage capabilities of terminal equipment and
- information collection from the terminal equipment

In general, the processing prohibition with permission reservation applies here as well. Pursuant to Article 8 para 1 lit. (a) – (d), the processing is permitted if:

- it is **necessary for the sole purpose of carrying out the transmission** of an electronic communication over an electronic communications network
- the end-user has given **consent**
- it is **necessary for providing an information society service requested** by the end-user
- it is necessary for **web audience measuring**
  - with the additional requirement that such measurement is **carried out by the provider of the information society service requested** by the end-user.

Aside from consent, all other permissions strongly focus on the principle of necessity to achieve the mentioned purposes. But this viewpoint of the EU lawmakers ignores the fact that nowadays, many technical communication standards compulsorily presuppose the transmission of data from the end-user's terminal equipment. Examples are the transmission of an IP address when going into the internet and surfing to a website, or additional information about the operating system, browser, plug-ins, or device type to optimally display such a website e. g. in the format of a mobile screen. Therefore, it must be assumed that the initial, technically required transmission must be understood as being allowed while the further processing of this information falls within the application scope of Article 8 draft ePR, while the necessity question might under circumstances remain difficult.[97] For consent requests and grants, Article 9 para. 2 allows to use '*where technically possible and feasible, […] the appropriate technical settings of a software application enabling access to the internet.'*

Paragraph 2 of Article 8 foresees permissions for the '*collection of information emitted by terminal equipment to enable it to connect to another device and, or to network equipment*'. This concerns the so-called **offline-tracking**, where the geo-location of mobile devices e.g. by WiFi or Bluetooth signals is being captured. Here, permissible processing is given if:

- it is done exclusively to establish a connection for the time necessary
- a clear and prominent notice is displayed, giving information about at least:
  - modalities of the collection,
  - purpose of collection,
  - person responsible,
  - other information required according to Article 13 GDPR,
  - measures the end-user of the terminal equipment can take to stop or minimise the collection

[97] See Engeler, M., Felber, W., '*Entwurf der ePrivacy-VO aus Perspektive der aufsichtsbehördlichen Praxis*', ZD 6/2017, p. 255 for more in-depth analysis of the technical implications.

Especially the last information obligation makes clear that the draft-ePR makes an opt-out approach to offline-tracking permissible. Therefore, the draft ePR has been heavily criticized as not having such a strong privacy by design and default focus like the GDPR.[98]

(c) Permissions addressing publicly available directories (Article 15)

Article 15 draft ePR foresees that providers of publicly available directories may only include personal data of natural persons only with their consent, whereby:

- consent must be requested for each category of data and
- the information must be relevant for the purpose of the directory.

If the directory provides a search function, end-user's consent is required prior to enabling the search. End-users being legal persons have a right to object data use. All end-users must have possibilities to verify, correct and delete this data free of charge.

(d) Permissions addressing unsolicited communications for direct marketing (Article 16)

Pursuant to Article 16 para. 1-3 draft ePR, sending **unsolicited direct marketing communications** is possible if:

- The end-user (who must be a natural person) has given **consent**.
- Electronic **contact details** for electronic mail of the end user are **obtained in the context of a sale** of a product or service **and** the **direct marketing is for** the provider's **own similar products or services**
  - the end-user must have an **opportunity to object** free of charge and in an easy manner and
  - this opportunity must be given at time of collection and each time a message is sent.
- In case of **direct marketing calls**,
  - a **contact line identity must be provided** and
  - a specific **code/or prefix identifying the call as a marketing call** must be provided

For all of the above possibilities, paragraph 6 foresees that information must be given about

- the marketing nature of the communication,
- the identity of the legal or natural person on behalf of whom the communication is transmitted,
- the necessary information for recipients to exercise their right to withdraw their consent.

Reflecting on all above described legal grounds for processing of electronic communications data in the draft ePR, the strong focus on consent is notable. Consent appears as a 'magic bullet' while it is still not clear how the preconditions on free, informed and unambiguous consent can be fulfilled in practice. Moreover, the draft ePR shows significant inconsistencies especially regarding the question who must give consent.[99] The addressee of the consent request is not clear in many cases:

[98] Cf. the IPOL study, page 82.

[99] EDPS Opinion 6/2017, page 14; Article 29 Working Party, WP 247, page 3, 13; IPOL study, page 43.

- Only the end-users who are customers of the respective electronic communications providers? What about the communication partners of those end-users?
- What about cases in which end-users are not natural persons? Who needs to give consent when a company subscribes as 'user' to services while its employees would be 'end-users'?

All of the above cause at the moment great legal uncertainty and it remains to be seen whether the EU lawmakers react to the broad criticism coming from industry as well as from fundamental rights advocates.

2.3.4 Outlook on legislative process

The draft ePR is in cases of personal data involvement lex specialis in the domain of electronic communications, but it still has many cross-references to the GDPR. This is especially the case for some definitions and key provisions, e.g. for consent. As a result, it deems advisable to always read the draft ePR together with the GDPR. However, some differences remain, especially with regard to privacy by design and by default, whereas the draft-ePR is weaker regarding the level of protection for the personal information of individuals.

So far, the recitals promise much in terms of fundamental rights protection and user control, yet this appears not to be reflected in the legal framework itself while some found this draft faulty in terms of promoting user consent as kind of a 'magic bullet'.[100] Furthermore, uncertainty is caused for potential cases of overlaps with the GDPR, especially when it conflicts with rules of the draft ePR.

Therefore, it remains to be seen whether the Council and the Parliament propose changes to the current draft and how supervisory authorities enforce the new legal framework. The Study of the University of Amsterdam initiated by the European Parliament*, recommended '[…] that the EU lawmaker pays extra attention to four points; (i) location tracking; (ii) browsers and default settings; (iii) tracking walls; (iv) the confidentiality of communications. Regarding those topics, the ePrivacy proposal does not ensure sufficient protection of the right to privacy and confidentiality of communications. Some provisions in the ePrivacy proposal offer less protection than the GDPR.'*[101] Furthermore, the study presents key findings and recommendations, stating that:

> '*The ePrivacy proposal has good elements, but should be significantly amended to protect the right to privacy and confidentiality of communications.*
>
> - *Location tracking, such as Wi-Fi tracking, should only be allowed after people give their consent (with possibly a limited exception for anonymous people counting, if there are sufficient safeguards for privacy).*
> - *Browsers and similar software should be set to privacy by default. It should be made easier for people to give or refuse consent to online tracking, for instance by requiring companies to comply with the Do Not Track standard.*
> - *Tracking walls and similar take-it-or-leave-it choices regarding privacy should be banned, or banned in certain circumstances.*
> - *Companies should only be allowed to analyse people's communications, such as emails, phone conversation, or chats, or the related metadata, when all end-users give meaningful informed consent, subject to limited, narrow, and specific exceptions. The definition of metadata should be amended.*

[100] Cf. Opinion 6/2017 '*EDPS Opinion on the Proposal for a Regulation on Privacy and Electronic Communications (ePrivacy Regulation)*' by the European Data Protection Supervisor Giovanni Buttarelli, or the Article 29 Working Party, '*Opinion 03/2016 on the evaluation and review of the ePrivacy Directive (2002/58/EC)*', WP 240.

[101] IPOL study, from the executive summary, page 8.

- *Other provisions should also be clarified and amended.'*[102]

The leading entity at the European Parliament responsible for reviewing the commission proposal is the Committee on Civil Liberties, Justice and Home Affairs (LIBE committee). The committee's rapporteur in the legislative process of the draft ePR is Marju Lauristin who brought forward her recommendations for a positioning of the parliament on June 21st, 2017. These recommendations are presented in a draft report proposing major changes to the draft of the ePrivacy Regulation made by the European Commission.[103] In summary, this draft report said that in its current form, the draft ePR would actually lower the level of protection to the personal data of individuals.

Some exemplary (not conclusive) mentions of the amendments proposed to the European Parliament are:

- Remedy the reliance on the draft EECC by including own definitions to the ePR. Thereby, the report proposes adapted definitions to e.g. include and clarify:
  - that the material scope includes not only information related to the terminal equipment of end-users, but also to the processing of such equipment,[104]
  - the concept of metadata,[105]
  - that a '*user*' is a natural person whose electronic communication is also protected even when this person is not using a paid service,[106]
  - that the confidentiality of communication extends to terminal equipment and to machine-to-machine communication when related to a user,[107]
- Changes of Article 6 draft ePR to clarify the conditions for lawful interference on the right of confidentiality of communication, putting more emphasis on the requirement of necessity (when it '*is technically strictly necessary*') and stating the requirements of prior consent more clearly. [108]
- A prohibition that a service is made conditional on the consent of an individual processing of personal information and/or the use of storage capabilities of his or her terminal equipment that is not necessary for the provision of that service or functionality.[109]
- Prohibition of offline-tracking without prior consent.[110]
- In cases of offline-tracking with anonymised data, this data shall be used only for statistical counting. Opt-out possibilities must be effective.[111]
- Demand for privacy by design and by default instead of opt-out approach. This includes information of the user and provision of changing privacy setting upon installation.[112]

[102] Ibidem, page 14.

[103] Committee on Civil Liberties, Justice and Home Affairs (LIBE committee), '*Draft Report 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) (COM (2017)0010–C8-0009/2017 – 2017/0003(COD))*'.

[104] Ibidem, page 41.

[105] Ibidem, page 47.

[106] Ibidem, page 47.

[107] Ibidem, page 49.

[108] Ibidem, pages 50 ff.

[109] Ibidem, page 59.

[110] Ibidem, page 60.

[111] Ibidem, page 61 f.

[112] Ibidem, page 64 f.

- Changes in Article 16 for unsolicited communications for direct marketing purposes that demand prior consent of an end-user, clarify that withdrawal of that consent is possible at any time. Moreover, the proposed changes demand information of users how they can exercise their right to refuse further written or oral marketing message.[113]

As mentioned above, the list is not conclusive. Aside from the LIBE committee report, the other European Parliament committees involved in the legislative process issued own opinions as well. While partially not as data protection friendly as the LIBE report, these opinions, though more market-oriented, also criticized the legal inconsistency with the GDPR, the lack of focus on communication confidentiality, and the unclear definitions in the draft ePR.[114]

In any case, the vote on the draft LIBE report in the European Parliament is still pending and it remains to be seen whether and to which extent the European Parliament takes its recommendations into account . Since the time frame until May 2018 is very tight, it is to be expected that a reaction of the Council and the Parliament need to come soon, meaning that the SPECIAL project will closely observe the legislative process over the next months.

2.4 Other relevant instruments

In the context of the SPECIAL project, other legal instruments on European level or on national level (in the countries of the project's industry partners) could be relevant for the use-case-driven research and development work. One of them is the European Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive) addressing the security of network and information systems to ward off cybersecurity incidents.[115] Besides the two legal instruments GDPR and ePrivacy Regulation, this directive might play a role as it may provide legal grounds for security-purposed personal data collection and processing in the context of the use cases. Therefore, further legal research work SPECIAL project will take the NIS directive into account as well.

[113] Ibidem, page 70 f.

[114] Cf. the draft opinions of the Committee on Legal Affairs (rapporteur Axel Voss), page 3 f., of the Committee on Industry, Research and Energy (rapporteur: Kaja Kallas), page 3 f., and of the Committee on the Internal Market and Consumer Protection (rapporteur: Eva Maydell), page 3 f. The Committee on Environment, Public Health and Food Safety decided not to give an opinion.

[115] *Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union*, OJ L 194, 19.7.2016, p. 1–30.

[This page is left blank intentionally. It is followed by the legal analysis of the SPECIAL use cases]

3 SPECIAL Use Cases

The SPECIAL use cases include confidential information and cannot be made public at this time. Should you have any question, please contact:

- Our Finance and Administration Coordinator: Philippe Rohou at philippe.rohou@ercim.eu
- Our Technical Coordinator: Sabrina Kirrane at sabrina.kirrane@wu.ac.at

4 Conclusions and remarks

The reform of the European data protection framework has an all-encompassing effect on future preconditions for lawful personal data processing in the European Union. Thereby, the GDPR and the future ePrivacy Regulation are the central legal instruments for the collection and processing of personal information in the context of the SPECIAL use cases.

In this deliverable, the legal frame conditions of this European data protection framework, including the anticipatable upcoming ePrivacy framework for the protection of privacy in the electronic communications sector have been examined. The first part of the document has presented more general requirements which apply to all processing of personal information, whereas the second part of the document focuses more on the specific use cases of the SPECIAL project.

A special case is the current situation in the United Kingdom due to the withdrawal of the country of the European Union and the industry partner TR being located there. For the time being, the outcome of the EU exit negotiations is unknown, so the applicability of the new European data protection framework in the UK is unclear as well. However, in SPECIAL non-UK industry partners with their use cases are involved as well, while SPECIAL is a project funded by the commission's Horizon 2020 programme. Therefore, the compliance demands of the European legal framework are paramount to SPECIAL.

Due to some open issues and uncertainties regarding project's use cases, as well as regarding the outcome of the legislative process of the ePrivacy Regulation, this document can in part not provide conclusive legal requirements. This will be an on-going process, leading up to version 2 of this deliverable which will be due in month 15 (March 2018). Until then, the legal experts in SPECIAL will work closely together with the industry partners and the relevant technical experts in the consortium. This will be done with focus on clarifying the above mentioned open issues and developing effective and innovative solutions facilitating compliance with the legal requirements applicable in the respective use cases.

5 References

Note: URL addresses listed in the references section to point to the respective document sources originate from those which could be found on the Internet at the time of writing this report, i. e. were valid links at the appointed date of June 30th 2017. No guarantee is given that those URLs still function at the time of any recipient reading this document.

5.1 Legislation and policy documents

Convention for the Protection of Human Rights and Fundamental Freedoms

(European Convention on Human Rights, ECHR), ETS No.005

Available at:

http://www.echr.coe.int/pages/home.aspx?p=basictexts

Charter of Fundamental Rights of the European Union

OJ C 364, 18.12.2000, p. 1–22

Available at:

http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32000X1218(01)

Consolidated version of the Treaty on the Functioning of the European Union

OJ C 326, 26.10.2012, p. 47–390

Available at:

http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A12012E%2FTXT

Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community

Signed at Lisbon, 13 December 2007

OJ C 306, 17.12.2007, p. 1–271

Available at:

http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A12007L%2FTXT

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

OJ L 281, 23.11.1995, p. 31-50

Available at:

http://eur-lex.europa.eu/eli/dir/1995/46/oj

Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)

OJ L 201, 31/07/2002 P. 0037 – 0047

Available at:

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:en:HTML

Directive 2008/63/EC of 20 June 2008 on competition in the markets in telecommunications terminal equipment

OJ L 162, 21.6.2008, p. 20–26

Available at:

http://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX%3A32008L0063

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

OJ L 119, 4.5.2016, p. 1–88

Available at:

http://eur-lex.europa.eu/eli/reg/2016/679/oj

Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC

OJ L 141/73, 5.6.2015, p. 73-117

Available at:

http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32015L0849

Proposal for a Directive of the European Parliament and of the Council establishing the European Electronic Communications Code (Recast)

COM(2016) 590 final/2, Brussels, 12.10.2016

Available at:

http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=comnat:COM_2016_0590_FIN

European Data Protection Supervisor Giovanni Buttarelli

'*Meeting the challenges of big data*'

Opinion 7/2015, 19 November 2015

Available at:

https://edps.europa.eu/sites/edp/files/publication/15-11-19_big_data_en.pdf

European Data Protection Supervisor Giovanni Buttarelli

'*EDPS Opinion on the Proposal for a Regulation on Privacy and Electronic Communications (ePrivacy Regulation)*'

Opinion 6/2017, 24 April 2017

Available at:

https://edps.europa.eu/sites/edp/files/publication/17-04-24_eprivacy_en.pdf

European Union Agency for Fundamental Rights

'*Handbook on European Data Protection Law*'

Luxembourg, Publications Office of the European Union, 2014

Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions:

'*Safeguarding Privacy in a Connected World - A European Data Protection Framework for the 21st Century*'

COM (2012) 9 final

Brussels, 25.1.2012

Available at:

http://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:52012DC0009

Court of Justice of the European Union (CJEU)

Judgement of the Court (Second Chamber)

Patrick Breyer v. Bundesrepublik Deutschland (Federal Republic of Germany)

Case C−582/14 of 16th October 2016

Available at:

http://curia.europa.eu/juris/celex.jsf?celex=62014CJ0582&lang1=de&lang2=EN&type=TXT&ancre=

Court of Justice of the European Union (CJEU)

Judgement of the Court (Grand Chamber)

Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González ('Google Spain')

Case C-131/12 of 13 May 2014

Available at:

http://curia.europa.eu/juris/document/document_print.jsf?doclang=EN&docid=152065

Court of Justice of the European Union (CJEU)

Judgement of the Court (Third Chamber)

Weltimmo s.r.o. v Nemzeti Adatvédelmi és Információszabadság Hatóság ('Weltimmo')

Case C-230/14 of 1 October 2015

Available at:

http://curia.europa.eu/juris/document/document.jsf?docid=168944&doclang=EN

Court of Justice of the European Union (CJEU)

Judgement of the Court (Grand Chamber)

Tele2 Sverige AB and Watson

Joined cases C-203/15 and C-698/15 of 21 December 2016

Available at:

http://curia.europa.eu/juris/liste.jsf?num=C-203/15

European Parliament

Committee on Civil Liberties, Justice and Home Affairs (LIBE committee)

'*Draft Report 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) (COM(2017)0010–C8-0009/2017 – 2017/0003(COD))*'

2017/0003(COD) published 9.6.2017

Rapporteur: Marju Lauristin

Available at:

http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+COMPARL+PE-606.011+01+DOC+PDF+V0//EN&language=EN

European Parliament

Committee on Legal Affairs (JURI)

'*Draft Opinion of the Committee on Legal Affairs for the Committee on Civil Liberties, Justice and home Affairs 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) (COM (2017)0010 – C8-0009/2017 – 2017/0003(COD))*'

2017/0003(COD) published 6.6.2017

Rapporteur: Axel Voss

Available at:

http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-%2f%2fEP%2f%2fNONSGML%2bCOMPARL%2bPE-605.986%2b01%2bDOC%2bPDF%2bV0%2f%2fEN

European Parliament

Committee on Industry, Research and Energy (ITRE)

'*Draft Opinion of the Committee on Industry, Research and Energy for the Committee on Civil Liberties, Justice and Home Affairs 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) (COM (2017)0010 – C8-0009/2017 – 2017/0003(COD))*'

2017/0003(COD) published 22.5.2017

Rapporteur: Kaja Kallas

Available at:

http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-%2f%2fEP%2f%2fNONSGML%2bCOMPARL%2bPE-602.722%2b01%2bDOC%2bPDF%2bV0%2f%2fEN

European Parliament

Committee on the Internal Market and Consumer Protection (IMCO)

'*Draft Opinion of the Committee on the Internal Market and Consumer Protection for the Committee on Civil Liberties, Justice and Home Affairs 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) (COM (2017)0010 – C8-0009/2017 – 2017/0003(COD))*'

2017/0003(COD) published 29.5.2017

Rapporteur: Eva Maydell

Available at:

http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+COMPARL+PE-604.857+01+DOC+PDF+V0//EN&language=EN

German Federal Constitutional Court (in German: Volkszählungsurteil Bundesverfassungsgericht)

Census decision of 15th December 1983

Az.: 1 BvR 209, 269, 362, 420, 440, 484/83

English translation of core excerpts of the decision available at:

https://freiheitsfoo.de//files/2013/10/Census-Act.pdf

Landgericht Frankfurt am Main

Judgement of June 10th 2016

Verbraucherzentrale Nordrhein-Westfalen e.V. vs. Samsung Electronics GmbH

Az.: 2-03 O 364/15

Body of European Regulators for Electronic Communications

'*Report on OTT services*'

BoR (16) 35 of January 2016

Available at:

http://berec.europa.eu/eng/document_register/subject_matter/berec/reports/5751-berec-report-on-ott-services

European Telecommunications Standards Institute (ETSI)

'*Electronic Programme Guide (EPG); Protocol for a TV Guide using electronic data transmission*'

ETSI EN 300 707 V1.2.1 (2003-04) standard

Available at:

http://www.etsi.org/deliver/etsi_en/300700_300799/300707/01.02.01_60/en_300707v010201p.pdf

Financial Action Task Force (FATF)

'*International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation*'

February 2012, last updated October 2016

Available at:

http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf

5.2 Article 29 Working Party opinions and other documents

Article 29 Data Protection Working Party

'*Opinion 10/2004 on More Harmonised Information Provisions*'

WP100, adopted 25th November 2004

Available at:

http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2004/wp100_en.pdf

Article 29 Data Protection Working Party

'*Opinion 4/2007 on the concept of personal data*'

WP 136, adopted 20th of June 2007

Available at:

http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf

Article 29 Working Party

'*Opinion 1/2010 on the concepts of "controller" and "processor"*'

WP 169, adopted on 16 February 2010

Available at:

http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_en.pdf

Article 29 Working Party

'*Opinion 2/2010 on online behavioural advertising*'

WP 171, adopted on 22 June 2010

Available at:

http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp171_en.pdf

Article 29 Working Party

'*Opinion 15/2011 on the definition of consent*'

WP 187, adopted on 13 July 2011

Available at:

http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf

Article 29 Data Protection Working Party

Letter to the Commissioner for Home Affairs Ms. Cecilia Malmström regarding the Proposal for a Regulation establishing the European Border Surveillance System

Brussels, 12/06/2012

Just.c.3(2012)818031

Available at:

http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2012/20120612_letter_to_eurosur_en.pdf

Article 29 Working Party

'*Opinion 03/2013 on purpose limitation*'

WP 203, adopted 2nd of April 2013

Available at:

http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf

Article 29 Data Protection Working Party

'*Opinion 05/2014 on Anonymisation Techniques*'

WP216, adopted 10th of April 2014

Available at:

https://cnpd.public.lu/fr/publications/groupe-art29/wp216_en.pdf

Article 29 Working Party

'*Opinion 03/2016 on the evaluation and review of the ePrivacy Directive (2002/58/EC)*'

WP 240, adopted on 19 July 2016

Available at:

http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2016/wp240_en.pdf

Article 29 Working Party

'Opinion 01/2017 on the Proposed Regulation for the ePrivacy Regulation (2002/58/EC)'

WP 247, adopted on 4 April 2017

Available at:

http://ec.europa.eu/newsroom/document.cfm?doc_id=44103

Article 29 Working Party
'*Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679*'
WP 248, adopted on 4 April 2017
Available at:
http://ec.europa.eu/newsroom/document.cfm?doc_id=44137

5.3 Academic sources

Abrecht, J. P.; Jotzo, F.
'Das neue Datenschutzrecht der EU – Grundlagen / Gesetzgebungsverfahren / Synopse'
(translated: '*The New Data Protection Law of the EU – Basis /Legislative Process /Synopsis*')
Nomos publishing house, Baden-Baden 2017

Barbaro, M.; Zeller, T.
'*A Face Is Exposed for AOL Searcher No. 4417749*'
Article published in The New York Times August 9th 2006
Available at:
http://www.nytimes.com/2006/08/09/technology/09aol.html

Ehmann, E, Selmayr, M. (ed.)
'*DS-GVO – Datenschutz-Grundverordnung*'
C.H. Beck publishing house, Munich 2017

Engeler, M., Felber, W.
'*Entwurf der ePrivacy-VO aus Perspektive der aufsichtsbehördlichen Praxis*'
(The draft of the ePR from the perspective of DPA practice)
Zeitschrift für Datenverarbeitung (ZD) 6/2017, pages 251-257

Gola, P. (ed.)
'*Datenschutz-Grundverordnung – VO (EU) 2016/679, Kommentar*'
C.H. Beck publishing house, Munich, 2017
Available at:
HTTPS://BECK-ONLINE.BECK.DE/?VPATH=BIBDATA/KOMM/GOLASCHOMERUSKOBDSG_12/CONT/GOLASCHOMERUSKOBDSG%2EHTM

Kühling, J.; Buchner, B. (ed.)
'Datenschutzgrundverordnung – Kommentar'
(translated: '*General Data Protection Regulation – Commentary*')
C.H. Beck publishing house, Munich, 2017

Holtz, L.; Zwingelberg, H.; Hansen, M.
'Privacy Policy Icons'
Chapter in: 'Privacy and Identity Management for Life', pp 279-285, Springer, 2011,
Available at:
https://link.springer.com/chapter/10.1007%2F978-3-642-20317-6_15

Kindt, E. MüllerL. (ed.)
'*Biometrics in identity management*'
FIDIS Project Deliverable D3.10, 2007, pp 83 – 87
Available at:
http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp3-del3.10.biometrics_in_identity_management.pdf

Li, N.; Li, T.; Venkatasubramanian, S.
'*t-Closeness: Privacy Beyond k-Anonymity and l-Diversity*'
Article published in International Conference on Data engineering (ICDE)
Vol. 7, 2007
Available at:
https://www.cs.purdue.edu/homes/ninghui/papers/t_closeness_icde07.pdf

Paal, B. P.; Pauly, D. A.
'Datenschutz-Grundverordnung'
C. H. Beck publishing house, Munich 2017
Available at:
https://beck-online.beck.de/?vpath=bibdata/komm/PaalPaulyKoDSGVO_1/cont/PaalPaulyKoDSGVO%2Ehtm

Pormeister, K.
'The GDPR and Big Data: leading the way for Big Genetic Data?'
Proceedings of Annual Privacy Forum 2017
Vienna, 2017

Machanavajjhalaet, A.; Kifer, D.; Gehrke, J.; Venkitasubramaniam, M.
'*l-diversity: Privacy beyond k-anonymity*'
Article published in ACM Transactions on Knowledge Discovery from Data (TKDD)
Vol. 1, March 2007
Available at:
https://www.truststc.org/pubs/465/L%20Diversity%20Privacy.pdf

Samarati, P., Sweeney, L.

'*Protecting Privacy when disclosing information: k-Anonymity and its enforcement through generalization and Suppression*'

Paper publishing in the proceedings of the IEEE Symposium on Research in Security and Privacy (S&P)

May 1998, Oakland, CA

Available at:

https://epic.org/privacy/reidentification/Samarati_Sweeney_paper.pdf

Schantz, P.

'*Die Datenschutz-Grundverordnung – Beginn einer neuen Zeitrechnung im Datenschutzrecht*'

(translated: 'The General Data Protection Regulation – Start of a New Era')

Neue Juristische Wochenschrift (NJW) 2016, p. 1841-1847

Available at:

https://beck-online.beck.de

Strobel, D.

'*IMSI Catcher*'

Publication for the Ruhr-University Bochum, Chair for Communication Security

July 13th 2007

Ulessi, C.

'*EU: Draft ePrivacy Regulation set to pose "considerable burdens for companies"*'

Article published January 12th 2017 on Dataguidance.com

Available at:

http://www.dataguidance.com/eu-draft-eprivacy-regulation-set-pose-considerable-burdens-companies/

Ustaran, E.

'*UK to Align Itself with the GDPR Despite Brexit*'

Article written for the web blog of Hogan Lovells US LLP

June 21st 2017

Available at:

http://www.hldataprotection.com/2017/06/articles/international-eu-privacy/uk-to-align-itself-with-the-gdpr-despite-brexit/

Wolff, H.A., Brink, S. (ed.)

'*Beck'scher Online-Kommentar Datenschutzrecht*'

20th Edition, Munich 2018

Available at:

https://beck-online.beck.de/?vpath=bibdata/komm/beckok/cont/beckok%2Ehtm

Zuiderveen Borgesius, F. (Dr.) et al.

IviR Institute for Information Law, University of Amsterdam

'An Assessment of the Commission's Proposal on Privacy and Electronic Communications'

Study requested by LIBE Committee, commissioned and published by the European Parliament's Directorate General for internal Policies, Policy Department C: Citizen's Rights and Constitutional Affairs

1 June 2017

Available at:

http://www.europarl.europa.eu/RegData/etudes/STUD/2017/583152/IPOL_STU(2017)583152_EN.pdf

5.4 SPECIAL deliverables, reports and other reference documents

SPECIAL Deliverable D1.1

Use case scenarios V1

Participants:

P.A. Bonatti, J. Colbeck, F. De Meersman, R. Jacob, S. Kirrane, M. Kurze, M. Piekarska, R. Wenning, B. Whittam-Smith, H. Zwingelberg, E. Schlehahn

6 List of Tables

7 List of acronyms and abbreviations

BEREC	Body of European Regulators for Electronic Communications
CJEU	Court of Justice of the European Union
CoE	Council of Europe
DTAG	Deutsche Telekom AG
ECHR	Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights)
ECHR	European Convention of Human Rights
ECtHR	European Court of Human Rights
EDPS	European Data Protection Supervisor
EEA	European Economic Area
EFTA	European Free Trade Association
ePR	ePrivacy Regulation
ETSI	European Telecommunications Standards Institute
EU	European Union
FATF	Financial Action Task Force
LIBE committee	Committee on Civil Liberties, Justice and Home Affairs
OJ	Official Journal of the European Communities
OJ L […]	Official Journal of the European Communities – Legislation
OJ C […]	Official Journal of the European Communities – Information and notices
PEP	Politically Exposed Person
PETs	Privacy Enhancing Technologies
Rec	Recommendation
SMO	Senior Management Official
TEU	Treaty on European Union
TFEU	Treaty on the Functioning of the European Union
TR	Thomson Reuters
UBO	Ultimate Beneficial Owner
WTO	World Trade Organisation