Brinkhof

ADVOCATEN

STUDY

EPR vis-à-vis GDPR

A comparative analysis of the ePrivacy Regulation and the General Data Protection Regulation

Prepared by
Brinkhof Advocaten

Prepared for
Centre for Information Policy Leadership

authors	prof. dr. G.-J. Zwenne LLM, Quinten Kroes LLM & Joost van Eymeren LLM
date	19 July 2018
reference	GJZ/BR-410624

TABLE OF CONTENTS

1 INTRODUCTION AND EXECUTIVE SUMMARY 3

1.1 Scope and objective 3

1.2 Approach 5

2 GENERAL OBSERVATIONS 6

2.1 The relationship between the ePR and the GDPR (lex specialis vs. lex generalis) 6

2.2 End-user vs. data subject 7

2.3 Personal data vs. electronic communications data 9

2.4 The role of the ECS-provider under the GDPR 10

3 CONFIDENTIALITY OF ELECTRONIC COMMUNICATIONS DATA 11

3.1 The ePR-rules for processing electronic communications data 11

3.2 GDPR-rules for processing electronic communications data (or: what if only the GDPR were to apply) 14

3.3 Analysis: overlap and impact of the ePR 20

4 STORAGE AND ERASURE OF ELECTRONIC COMMUNICATIONS DATA 21

4.1 The ePR-rules on storage and erasure of electronic communications data 21

4.2 GDPR-rules on storage and erasure of electronic communications data (or: what if only the GDPR were to apply) 22

4.3 Analysis: overlap and impact of the ePR 23

5 PROTECTION OF INFORMATION STORED IN AND RELATED TO END-USERS' TERMINAL EQUIPMENT 24

5.1 The ePR-rules on protection of information on end-users' terminal equipment 24

5.2 GDPR-rules for data collection from terminal equipment (or: what if only the GDPR were to apply) 26

5.3 Analysis: Overlap and impact of the ePR 28

6 OBLIGATION ON ECS-PROVIDERS TO HELP END-USERS MAKE EFFECTIVE CHOICES ABOUT PRIVACY SETTINGS 30

6.1 The ePR-rules on information and options for privacy settings in software permitting electronic communications 30

6.2 GDPR-rules for information and options for privacy of electronic communications software (or: what if only the GDPR were to apply) 31

6.3 Analysis: overlap and impact of the ePR 32

7 USE CASES 33

7.1 Use case 1: Development of an AI support agent 33

7.2 Use case 2: Use of device fingerprinting for fraud prevention 35

8 GENERAL CONCLUSIONS 36

1 INTRODUCTION AND EXECUTIVE SUMMARY

1.1 Scope and objective

On 10 January 2017, the Commission adopted its proposal for a new ePrivacy Regulation[1] ("ePR") to replace the existing Directive 2002/58/EC. This proposal is currently being discussed in the Council. One of the questions being considered, is the link between the ePR and the General Data Protection Regulation ("GDPR").[2] In particular, the current Presidency has tabled the question whether clarification is needed on where the ePR complements the GDPR, and where it particularises it, with a focus on art. 5, 6, 7, 8 and 10 of the ePR.[3]

The objective of this short study is to get a better understanding of the relationship between the proposed ePR and the GDPR, and more specifically, to map where both instruments overlap and diverge.

To do so we will:

- summarise the meaning of each of the ePR-articles listed above;
- describe what protection the GDPR provides in absence of these ePR-articles;
- describe the link between the two regulations if the ePR were to be adopted as proposed by the Commission, including which regime will take precedence in the event of a conflict between the two; and
- identify what, if any, added value the ePR would bring over the GDPR.

We look at these effects of the ePR from the perspective of both the protection of fundamental rights and freedoms and the free movement of electronic communications data and electronic communications services within the Union.[4]

[1] 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), Brussels, 10.1.2017 COM(2017) 10 final2017/0003 (COD).

[2] 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* L199/1-87, 4.5.2016.

[3] Note from the Presidency of 11 January 2018 in file no. 2017/0003 (COD), 5165/18 (which we will refer to as: the "Council Note").

[4] The two objectives of art. 16 of the Treaty on the Functioning of the EU (TFEU).

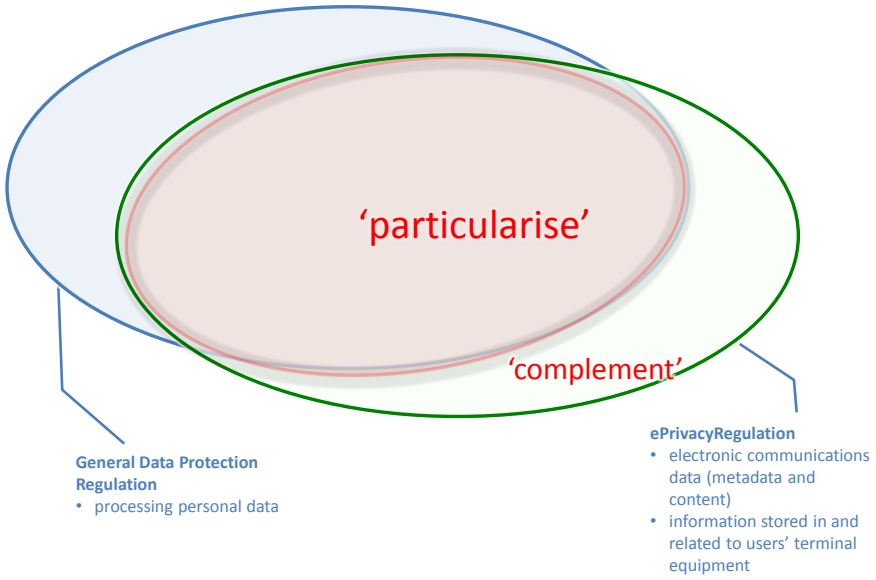

Figure 1 visual representation of the scope of the study

Figure 1 provides a visual representation of our study. In effect we are looking to establish how substantive the overlap is, and how substantive the remaining ePR 'circle' is.

Our findings can be summarised as follows:

- the ePR intends to <u>particularise</u> the rules of the GDPR insofar as it relates to processing of data that qualify as personal data;
  - however, it does not always succeed in this aim, because it does not actually complement, add to, or deviate from the GDPR in any meaningful way;
  - where the ePR does add to or deviate from the GDPR, it is unclear what the added value is, either in terms of enhancing data protection rights, or supporting the free movement of data and services;
  - in particular, there is an overreliance on 'consent' as a legal basis for data processing, which would exclude alternative legal bases permitted under the GDPR, like the need to process data for the purposes of a 'legitimate interest';
- the ePR also intends to <u>complement</u> the rules of the GDPR, where the latter clearly does not apply, for example when it comes to data concerning legal persons;
  - however, the ePR's added value here may also be marginal, as these data will in most cases also relate to natural persons;

- moreover, the usefulness of covering legal persons by ePR-rules is limited as it will be problematic in practice to apply concepts like consent to legal persons; and
- more fundamentally, one can question the suitability of applying the concept of privacy to corporate communications data (which is not personal data), especially in light of the fact that such corporate data will also enjoy protection under rules such as those contained in the Council of Europe's Convention of Cybercrime.

1.2 Approach

This study aims to be concise. We do not aim to give a full and detailed analysis of the ePR and the GDPR, but merely to point out unnecessary overlap and inconsistencies of both regulations.

Given the question raised by the current Presidency (as discussed in para. 1.1), our focus will be specifically on the following provisions from the ePR:

- chapter 3: the principle of confidentiality of electronic communications (art. 5 ePR) and its exemptions (i.e. permitted processing of electronic communications data; art. 6 ePR);
- chapter 4: storage and erasure of electronic communications data (art. 7 ePR);
- chapter 5: protection of information stored in and related to end-users' terminal equipment (art. 8 ePR); and finally
- chapter 6: information and options for privacy settings to be provided (art. 10 ePR).

For each of these provisions we apply the following approach:

- we begin by *summarising* the ePR provisions;
- we then *map* the corresponding relevant provisions of the GDPR (answering the question: what if only the GDPR were to apply); and
- we will then go on to compare these and identify how the ePR-provision particularises and/or complements the relevant GDPR-provisions: to what extent does our comparison show inconsistencies or other problematic issues?

Before our discussion of each of these specific ePR-provisions we will begin by making some general observations (chapter 2).

We will end our analysis by illustrating our findings in more concrete terms by applying them at a more practical level to a *use-case* (chapter 7).

2 GENERAL OBSERVATIONS

We begin our analysis with a number of general observations regarding the ePR and the GDPR, which should help our more specific analysis of the ePR-provisions in the chapters that follow:

- para. 2.1 addresses the relationship between the ePR on the one hand and the GDPR on the other;
- para. 2.2 looks at who is protected by each regulation, i.e. the end-user and subscriber (ePR), and the data-subject (GDPR);
- para. 2.3 looks at the type of data that is subject to regulation, electronic communications service ("ECS")-data vs. personal data; and
- para. 2.4 will assess the role of the ECS-provider under the GDPR (controller or processor).

2.1 The relationship between the ePR and the GDPR (lex specialis vs. lex generalis)

According to art. 1.3 and recital 5 ePR, the ePR-provisions are intended to 'particularise and complement' the GDPR by laying down specific rules. These specific rules should serve the dual purposes of (1) protecting the fundamental rights and freedoms of natural and legal persons in the provision and use of electronic communications services (art. 1.1 ePR) and 1.2 ensuring free movement of electronic communications data and electronic communications services within the Union (art. 1.2 ePR). The Commission has confirmed that all matters concerning the processing of personal data that are not specifically addressed by its ePR-proposal, are covered by the GDPR.[5]

So in short, we can distinguish the following three categories (as also shown in Figure 1):

1 matters to which only the GDPR applies: processing of personal data not specifically addressed by the ePR;

2 matters where the ePR takes precedence over the GDPR: processing of personal data where the ePR particularises the GDPR by imposing more specific rules;

3 matters where only the ePR applies: processing of data which are not personal data, where the ePR complements the GDPR, by extending protection to end-users which are legal persons.

[5] Explanatory Memorandum to the ePR, para. 1.2.

To better understand the relative importance of these three categories, we will now look at some of the key concepts which determine this, i.e. end-users vs. data subjects (para. 2.2), and personal data vs. electronic communications data (para. 2.3).

2.2 End-user vs. data subject

Many of the ePR-provisions refer to the end-user and give the end-user the right to control the processing of data which is generated in the context of the electronic communication services.

The *end-user* is defined, in short, as an individual or legal entity that actually uses an electronic communications service.[6] This concept deviates from the ones used in the current e-Privacy Directive,[7] which instead refers to *subscribers* and *users*. The ePR concept of end-user of course also deviates from the concept of *data subject*, which the GDPR aims to protect.

DEFINITIONS: USER, SUBSCRIBER (E-PRIVACY DIRECTIVE), END-USER (EPR) AND DATA SUBJECT (GDPR)		
User	*natural person using a publicly available electronic communications service, for private or business purposes, without necessarily having subscribed to this service*	*Art. 2(a) e-Privacy Directive*
Subscriber	*natural person or legal entity who or which is party to a contract with the provider of publicly available electronic communications services for the supply of such service*	*Art. 2(k) Framework Directive*[8]
End-user	*legal entity or natural person using or requesting a publicly available electronic communications service, not providing public communications networks or publicly available electronic communications services.*	*Art. 1(b) ePR*
Data subject	*An identified or identifiable natural person, with identifiable meaning that such person 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.*	*Art. 4.1 GDPR*

Table 1

[6] Art. 4.13 proposal for a directive of the European Parliament and of the Council establishing the European Electronic Communications Code.

[7] 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).

[8] Directive 2002/21/EC Of The European Parliament And Of The Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive).

At least in theory, the differences between the concept of *end-user* (ePR) and *data subject* (GDPR) result in the ePR having a broader application, as it protects the privacy of both individuals and legal persons who use electronic communications services.

Recital 3 ePR confirms that this is indeed intended, as it states that where reference is made to consent by an end-user, this should include legal persons. It also explains that this is considered necessary because electronic communications data may reveal economically sensitive information data about legal entities, such as business secrets and other economically valuable information.

This is a marked departure from the original e-Privacy Directive, which was aimed at *protecting the fundamental rights of natural persons* by supplementing Directive 95/46/EC, but did not entail an obligation for Member States to extend the application of Directive 95/46/EC to the protection of the interests of legal persons, for instance to ensure confidentiality of communications.

At the time that the e-Privacy Directive was adopted in 2002, an extension of its scope to legal persons was expressly rejected, as this was considered already sufficiently ensured within the framework of the applicable Community and national legislation.[9] If this was a valid consideration then, it is even more so now, given legislative initiatives which have become part of the Union's and Member States' legal frameworks since, like the Council of Europe's Convention On Cybercrime,[10] and, more recently, the Directive on trade secrets[11] and the NIS Directive,[12] as well as other legislative initiatives aimed at protection data security and trust, such as the eIDAS Regulation.[13]

This raises valid questions about the need to expand the scope of ePR-protections to legal persons. Where a legal entity purchases an electronic communications service which is used by its employees, should the provider of this ECS (the "ECS-provider") seek consent from both the legal entity and the employees,[14] as they both qualify as persons using or requesting the service? And what is the added value of having consent from both categories of end-users?

---

[9] Recital 12 of the e-Privacy Directive.

[10] Convention of Cybercrime of 23 November 2001, European Treaty Series No. 185.

[11] Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure.

[12] Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union.

[13] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

[14] In an employer-employee relationship consent is generally problematic, because of the dependency that results from the employer-employee relationship. See recital 43 GDPR, and WP259, p. 7.

Practically, an ECS-provider may only be able to obtain one, but not both. For example, an ECS-provider providing telephony-services to a multinational company, may be able to secure consent from the company, but not from each individual employee. Conversely, a provider of ECS-hardware or -software used in a corporate setting, may be able to obtain consent from individual employees who use their device or app, but not from the company. It is unclear whether these scenarios will qualify as sufficient forms of end-user consent. The meaning of consent for end-users should therefore be clarified. This could entail that the consent of the legal entity through the consent of one employee duly authorised to act on its behalf should be sufficient.

Moreover, as we will see in the discussion of specific provisions, this broader application of the ePR may be insignificant in practice, as electronic communications services are ultimately used by individuals, even if these services are being purchased by legal entities. This will likely bring data generated within the context of the provision of electronic communications services within the scope of the GDPR anyway, because these will qualify as personal data in most cases, as the next paragraph will explain.

2.3 Personal data vs. electronic communications data

Another, somewhat related difference between the ePR and the GDPR, is that while the GDPR regulates processing of *personal data*, the ePR uses different data concepts, like *electronic communications data* (art. 7 and 8 ePR) and *information stored in and related to end-users' terminal equipment*. Like personal data, electronic communications data is a defined term. The meaning of these definitions is set out below.

<table>
<tr><th colspan="2">RELEVANT DEFINITIONS</th></tr>
<tr><th>ePR</th><th>GDPR</th></tr>
<tr><td>Electronic communications data: art. 4.3(a)
Electronic communications content and electronic communications metadata</td><td rowspan="4">Personal data: art. 4.1
Any information relating to an identified or identifiable natural person (data subject)

Recital 30:
Natural persons may be associated with online identifiers provided by their devices, applications, tools and protocols, such as internet protocol addresses, cookie identifiers or other identifiers such as radio frequency identification tags. This may leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them.</td></tr>
<tr><td>Electronic communications content: art. 4.3(b)
content exchanged by means of electronic communications services, such as text, voice, videos, images, and sound</td></tr>
<tr><td>Electronic communications metadata art. 4.3(c)
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</td></tr>
</table>

location of the device generated in the context of providing electronic communications services, and the date, time, duration and the type of communication	

Table 2

Again, in theory, the ePR could be said to complement the GDPR and have a broader application, in that it regulates the processing of electronic communications data, even if this does not relate to an identified or identifiable natural person. But here, too, this is unlikely to make a significant difference in practice. This is because ultimately most electronic communications relevant to this study still take place *between individuals*. As a result, most electronic communications data can be related to one or more data subjects, and will qualify as personal data, bearing in mind that the concept of personal data should be interpreted broadly, and may include unique identifiers (like an IP-address) which may be used to identify someone.[15]

A possible exception, which may grow more important in the near future, is M2M communication. But even there, in many instances such communications will have a link to an identifiable natural person (e.g. the driver of a car with a telematics device, or the consumer who owns an alarm-system) and may qualify as personal data. This has been confirmed by the Art. 29 Working Party ("WP29") in its opinion on the Internet of Things,[16] where it considered that it is often the case that an individual can be identified based on data that originates from "things", and that machines which are used to collect and further process an individual's data[17] *should be deemed equipment used for the purpose of processing personal data*.

This leaves only a small subset of pure M2M communications relating to purely industrial processes which do not involve or centre around specific humans (e.g. remote monitoring of fully automated industrial equipment). While it is true that the ePR may apply to data generated in such settings, whereas the GDPR does not, it could be argued that there are no real privacy issues at stake there which warrant regulation and are not already adequately addressed by existing rules against hacking, cybercrime and unlawful interception (see para. 2.2).

2.4 The role of the ECS-provider under the GDPR

The GDPR imposes obligations on controllers on the one hand and, to a lesser extent, processors on the other.

[15] This is true even if identification requires additional information from a third party which may be obtained by legal means, see CJEU 19 October 2016 (Breyer), ECLI:EU:C:2016:779.

[16] Opinion 8/2014 on the on Recent Developments on the Internet of Things, WP223.

[17] The art. 29 Working Party mentions step-counters, sleep trackers, "connected" home devices like thermostats, smoke alarms, and connected glasses or watches, as well as data generated by the centralised control of lighting, heating, ventilation and air conditioning for an individual or family.

The controller is defined as the natural or legal person which alone or jointly with others determines the purpose and means of the processing of personal data. Processor refers to a natural or legal person, which processes personal data on behalf of the controller.

When it comes to the processing of electronic communications *metadata*, it is clear that ECS-providers will qualify as controllers.[18] Their qualification when processing electronic communications *content* is less obvious. WP29 suggests that telecom-operators qualify as processors for *any* data being transmitted ('data in transit').

However, for electronic communications content 'at rest', the analysis may be more complicated. For example, an email operator which hosts copies of email messages on behalf of its customers will generally qualify as a processor.[19] But WP29's more recent paper on data portability[20] suggests that a webmail service should be considered a data controller when it comes to storage of a directory of a data subject's contacts, friends, relatives, family and broader environment and the entire directory of incoming and outgoing e-mails to the data subject. Ultimately, this may also depend on the circumstances. For example, an ECS-provider processing electronic communications content at rest for its own purposes (e.g. an email provider which scans the content of email messages to display relevant ads) will qualify as a controller.

Whichever of these approaches may apply, it is clear that an ECS-provider will have to observe the GDPR when processing personal data, either as a controller, or as a processor for its customers.

3 CONFIDENTIALITY OF ELECTRONIC COMMUNICATIONS DATA

3.1 The ePR-rules for processing electronic communications data

In the context of the provision of electronic communications services, an ECS-provider will process electronic communications data, which comprise the following two subcategories (as set out in Table 1):

- *content*, such as text, voice, videos, images, and sound; and
- *metadata*, like the 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 the services, as well as the date, time, duration and the type of communication.

[18] Recital 47 to Directive 95/46/EC.

[19] Opinion 1/2010 on the concepts of "controller" and "processor", WP169, 16 February 2010, p. 11 and 25.

[20] Guidelines on the right to data portability, WP242.

This chapter will first describe what will, and what won't be allowed with respect to electronic communications data, pursuant to art. 5 and 6 ePR. We then go on to analyse what is allowed under the GDPR, in the absence of the specific ePR-rules.

3.1.1 *General rule: confidentiality of metadata and content (art. 5 ePR)*

Metadata and content are to be kept confidential. The general rule is that any interference with the data by persons other than the end-users is prohibited, except when explicitly permitted by the ePR. In other words, an ECS-provider, or any other party, is not allowed to listen, tap, store, monitor, scan or intercept, or process in any other way electronic communications data, i.e. metadata and content (art. 5 ePR).

Obviously, the ePR does provide for a number of exemptions for processing metadata and content, as described in the following paragraphs.

3.1.2 *Exemptions for using both metadata and content: permitted use by the ECS-provider (art. 6.1(a) ePR (transmission) and 6.1(b) ePR (security))*

ECS-providers may process both metadata and content to provide their electronic communications services. They can use those data if, and only to the extent that, the data are necessary for the transmission of the communication, or to maintain or restore the security of the services and networks.

PROCESSING ELECTRONIC COMMUNICATIONS DATA (art. 6.1 ePR)		
purpose of processing	**main requirement**	**other specific requirements**
providing ECS	*necessary for provision of a secure service*	--
maintaining security of networks and services		

Table 3

3.1.3 *Exemption: use of metadata to meet Quality-of-Service-requirements and billing purposes and the like*

Metadata (but not content data) may be used by an ECS-provider in order to meet mandatory Quality-of-Service ("QoS")-requirements or for billing purposes, calculation of interconnection payments, detection and stopping fraudulent or abusive use of, or subscription to the services.

PROCESSING METADATA (art. 6.2(a)-(b) ePR)		
purpose of processing	**main requirement**	**other specific requirements**
quality of service-requirements, billing purposes, calculation of interconnection payments, detection and stopping	*Processing must be necessary for these purposes*	--

fraudulent or abusive use of the services, etc.		

Table 4

3.1.4 *Exemption: use of metadata to provide 'specific services' to end-users (art. 6.2(c))*

ECS-providers may also use metadata for specific purposes, including the provision of specific services to the relevant end-user, provided that the end-user has consented to this, and that this cannot be done with anonymous data. The regulation is not clear on the nature of such types of services. Recital 18 suggests these services include 'advertisements' and 'protection services against fraudulent activities, by analysing usage data, location and customer account in real time'. Supposedly, an end-user could choose the first type of service to obtain ad-funded discounted or free services, and the second type of service to detect fraud with expensive toll numbers or to prevent bill-shock.

PROCESSING METADATA (art. 6.2(c) ePR)		
purpose of processing	**main requirement**	**other specific requirements**
specific services e.g. fraud protection services on the basis of real-time metadata analysis	*end-user consent*	*cannot be done with anonymous data*

Table 5

3.1.5 *Exemption: use of content data for specific service or specified purpose (art. 6.3 ePR)*

An ECS-provider may process electronic communications content to provide a service that is *specifically requested*[21] by the end-user, provided that (i) this end-user has consented to such processing and (ii) the service cannot be provided without processing the content. Again, here the regulation is not very clear on the type of services the article refers to. The fact that consent is required from only the end-user that has requested the service (rather than from all end-users participating in a communication), suggests that the article is intended to apply to communications between an end-user and the ECS-provider, but *not to communications between end-users*. Examples might include intelligent assistant services or (outbound) text-to-speech services offered by the ECS-provider.

The requirement that the service must be specifically requested, raises questions for the situation where a service is rolled out as a new feature of an existing service. Arguably, this business model is not allowed, even with the consent of the user, as the new feature would not be specifically requested by the end-user.

[21] This requirement is not included in art. 6.3(a) ePR but is mentioned in recital 19.

An ECS-provider may also process content for *specified purposes*, provided that (i) all end-users (which would seem to comprise all participants in a communication) have consented to this, (ii) these purposes cannot be attained with anonymous data, and (iii) the competent supervisory authority has been consulted. Recital 19 ePR suggests that this is relevant for content filtering, like, for example, services that entail the scanning of emails to remove certain pre-defined material. This recital also explains that such services are presumed to result in high risks to the rights and freedoms of natural persons (all end-users) and therefore, pursuant to art. 6.3(b) ePR, the supervisory authority should be consulted prior to the processing.

PROCESSING CONTENT (art. 6.3(a)-(b) ePR)		
purpose of processing	**main requirement**	**other requirements**
providing specifically requested services (e.g. indexing, text to speech) to end-user	*end-user consent (of the end-user requesting the service)*	*cannot be done without processing content*
for specified purposes (e.g. removal of specific content)	*end-user consent (of all end-users)*	*cannot be done with anonymous data* *prior supervisory authority consultation*

Table 6

3.2 GDPR-rules for processing electronic communications data (or: what if only the GDPR were to apply)

What is an ECS-provider allowed to do with electronic communications data (metadata and content), if only the GDPR were to apply? And what is an ECS-provider *not* allowed to do? To answer these questions, we will assume (for the sake of simplicity) that the end-user is a natural person, who is identified or identifiable (a data subject; see Table 1). This implies that the electronic communications data qualify as personal data, the processing of which must comply with the GDPR.

3.2.1 *General GDPR rules: legal basis for processing, principles relating to processing*

One of the essential requirements of the GDPR is that processing of personal data may only take place if there is a sufficient legal basis. Art. 6 GDPR lists these grounds for lawful processing, which include the following:

- Consent: the data subject has given consent to the processing for one or more specific purposes, with consent meeting all the requirements of art. 4.11, 7 and 8 GDPR;

- A contract with the data subject: 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;
- A legal obligation: processing is necessary for compliance with a legal obligation to which the controller is subject; and
- A legitimate interest: 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 ('legitimate interest').

Other essential principles of EU data protection law are set out in art. 5 GDPR. These include the following:

- purpose limitation;
- data minimisation;
- integrity and confidentiality; and
- storage limitation.

The following table gives a full summary of the legal bases and processing principles of the GDPR.

RELEVANT GDPR PRINCIPLES	
GDPR legal basis (art. 6.1 GDPR)	*GDPR processing principles (art. 5 GDPR)*
a. consent b. contract with the data subject c. legal obligation of the controller d. vital interest of a natural person e. public interest or official authority f. legitimate interest	1.a lawfulness, fairness and transparency 1.b purpose limitation 1.c data minimisation 1.d accuracy 1.e storage limitation 1.f integrity and confidentiality 2. accountability

Table 7

3.2.2 *Confidentiality of electronic communications data (GDPR)*

The GDPR imposes a general obligation to protect personal data against unauthorised or unlawful processing (art. 5.1(f)), which is further fleshed out in section 2 of Chapter IV. This includes an obligation for controllers and processors to take measures to ensure the ongoing confidentiality of processing systems and services (art. 32.1(b) GDPR). They must also ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality (art. 28.3(b), art. 29 GDPR).

3.2.3 *Processing metadata and content to provide electronic communications services and maintain network security (GDPR)*

Processing of metadata and content to provide the services and maintain network security is allowed under the GDPR, either because it is necessary for the contract with the end-user (if the end-user is a natural person) or because there is a legitimate interest (if the end-user is a legal person[22]).

Examples are the set-up of a mobile or fixed call which requires the devices used by the caller and recipient of the call to be identified and their locations to be determined, as well as the type of communication that is transmitted (e.g. call, text or data). In order to provide a reliable service and maintain network security, and to prevent or resolve congestions problems, the processing of metadata will be allowed, e.g. in case of trouble-shooting by a customer-care agent but also if a device malfunctions and/or hampers or interferes with the communication of other end-users.

When it comes to processing of electronic communications data to maintain or restore the security of electronic communications networks and services, ECS-providers may also be able to rely on their legal obligation as controller under the GDPR to maintain the security and confidentiality of their networks, as the legal basis for their data processing.

Of the GDPR's processing principles, the data minimisation requirement is probably the one most pertinent for the comparison to the ePR. To comply with the data minimisation requirement, an ECS-provider will have to ensure the data used are adequate, relevant and limited to what is necessary in relation to those purposes (art. 5.1(c) GDPR).

[22] In Opinion 2/2017 on data processing at work (WP249), WP29 considered that monitoring of employee communication should rely on the legitimate interest basis, and illustrated how this test should be applied (p. 24 and example 14).

PROCESSING ELECTRONIC COMMUNICATIONS DATA FOR TRANSMISSION, SECURITY (GDPR)		
purpose of processing	**main requirement**	**other requirements**
providing ECS	*legal basis:* *performance of contract (for* subscriber/natural person) *legitimate interests* *consent*	*data minimisation*
maintain security	*legal basis:* *performance of contract (for subscriber/natural person)* *legitimate interests* *legal obligation* *consent*	*data minimisation*

Table 8

3.2.4 *Processing metadata to comply with QoS-requirements, billing etc. (GDPR)*

Services provided to end-users should comply with mandatory QoS-standards. The processing of their metadata for these purposes may be considered necessary to comply with a legal obligation of the ECS-provider.

Processing of metadata for billing and other related purposes is necessary for the performance of the agreement. As we saw above, the legal basis for this will depend on whether the subscriber of the service is an individual or a legal entity. For the former, the ECS-provider can rely on the contract with the data subject as a legal basis, for the latter, it will be able to rely on its legitimate interests (or consent of the end-user).

In accordance with the data minimisation principle, all metadata used should be adequate, relevant and limited to what is necessary in relation to the purposes of meeting QoS-requirement, performing billing etc.

PROCESSING METADATA FOR QOS REQUIREMENTS, BILLING (GDPR)		
purpose of processing	**main requirement**	**other requirements**
mandatory QoS requirements	*legal obligation*	*data minimisation*
billing, calculating interconnection payments, detecting fraud, etc.	*performance of contract (for* subscriber/natural person) *legitimate interests* *consent*	*data minimisation*

Table 9

3.2.5 *Processing metadata to provide specific services (e.g. real time analysis fraud protection) (GDPR)*

With respect to the provision of specific services, such as fraud protection services on the basis of real-time metadata analysis, the GDPR does not necessarily require the consent of the end-user. Under the GDPR, other processing grounds or legal bases on which an ECS provider could rely, are the performance of a contract, and the legitimate interests.

The GDPR demands that personal data is collected only for specified, explicit and legitimate purposes (purpose specification) and not further processed in a manner that is incompatible with those purposes (purpose limitation).[23] The processing of metadata (which were originally collected to provide the ECS, and perform billing and related support) to provide specific services will have to comply with the principle of purpose limitation. In concrete terms this means that the ECS provider will have to consider the relationship or link between the original collection and further processing purposes, the context in which the data were collected, the nature of the data, possible consequences for the data subject and the availability of appropriate safeguards.[24] Depending on the privacy-impact and user-expectations, a specific service may or may not meet the purpose limitation test. If not, an ECS-provider may need to obtain consent for the service.[25] Alternatively, the provider will need to find a new basis for processing (including, maybe, consent) and notify the data subject of the new purpose and the new basis for processing.

To comply with data minimisation requirements the ECS-provider will have to ensure personal data included in the metadata and content used are adequate, relevant and limited to what is necessary in relation to those purposes (art. 5.1(c) GDPR). If the services can be provided on the basis of less personal data, or even anonymous data, the ECS-provider will have to choose those options.

PROCESSING METADATA FOR SPECIFIC SERVICES (GDPR)		
purpose of processing	**main requirement**	**other requirements**
specific services e.g. fraud protection services on the basis of real-time metadata analysis, provided to end-user subscriber	*performance of contract (for* subscriber/natural person) *legitimate interests* *consent*	*purpose compatibility test* *data minimisation*

Table 10

[23] Art. 5.1(b) GDPR, see also Opinion 03/2013 on purpose limitation, WP203.

[24] Art. 6.4(a)-(e) GDPR.

[25] Art. 6.4 GDPR.

3.2.6 *Processing content for specifically requested services (GDPR)*

Under the GDPR, if the subscriber to the services is an individual, the legal basis for processing content to provide specifically requested services most likely will be the performance of the contract (art. 6.1(b) GDPR). In other cases, ECS-providers will be able to rely on their legitimate interests (art. 6.1(f) GDPR), or on the end-users' consent. Whether a controller is able to rely on a legitimate interest, will to an important extent depend on the impact of the processing on the rights and interests of the data subject. If this impact is significant and cannot be reduced with safeguards like aggregation or anonymisation techniques,[26] the controller may not be able to rely on legitimate interest as a legal basis, and user consent may need to be obtained.

Moreover, as in the abovementioned example of the fraud protection services, a purpose compatibility test will have to be done (art. 5.1(b) and 6.4 GDPR). Furthermore, to comply with data minimisation requirements the metadata will have to be relevant and limited to what is necessary in relation to the purpose of providing the services (art. 5.1(c) GDPR). Consequently, the ECS-provider may not process content data if the service can also be provided without the additional service requiring the processing of content data.

If the processing to be undertaken by the ECS-provider is likely to result in a high risk to the rights and freedoms of natural persons (which could also include individuals who are not end-users), particularly as a result of the application of new technologies, a data protection impact assessment (DPIA) will need to be undertaken (art. 35 GDPR). If this assessment indicates that processing would result in a high risk, the ECS-provider will have to consult the supervisory authority (art. 36 GDPR).

PROCESSING CONTENT FOR SPECIFICALLY REQUESTED SERVICES (GDPR)		
purpose of processing	**main requirement**	**other requirements**
specifically requested services, e.g. intelligent assistant service or text-to-speech	*performance of contract (for* subscriber/natural person) *legitimate interests* *consent*	*purpose compatibility test* *data minimisation* *depending on the risk: DPIA and prior consultation*

Table 11

3.2.7 *Processing content for specified purposes (GDPR)*

With respect to the use of content for specified purposes, such as filtering content like the scanning of emails to remove certain pre-defined material, the ECS-provider is able to rely on the same legal bases as for specifically requested

[26] WP29's Opinion 06/2014 on the notion of legitimate interests of the data controller under rt. 7 of Directive 95/46/EC (WP217), p. 30, 31.

services, but may also be able to rely on a legal obligation where filtering is required by Union or Member State law (as may be the case for hate speech or other illegal content). Where filtering is not mandated by law, it may still be permitted if it is carried out in the public interest (art. 6.1 e GDPR).

If the intended processing is likely to result in a high risk to the rights and freedoms of natural persons, it may be necessary to undertake a DPIA and consult the supervisory authority beforehand.

PROCESSING CONTENT FOR SPECIFIED PURPOSES (GDPR)		
purpose of processing	**main requirement**	**other requirements**
specified purposes that cannot be fulfilled by processing information that is made anonymous	*performance of contract (for* subscriber/natural person) *legitimate interests* *legal obligation* *public interest* *consent*	*purpose compatibility test* *data minimisation* *depending on the risk: DPIA and prior consultation*

Table 12

3.3 Analysis: overlap and impact of the ePR

3.3.1 *Overlap*

- The GDPR may not have a general prohibition on interference with electronic communications, but does have strict and detailed rules to secure the confidentiality of personal data. In this respect, the added value of the ePR for electronic communications data which also constitute personal data is small.

- Processing of electronic communications data (both metadata or content) is only allowed under the ePR for the provision of an ECS and to maintain or restore the security of the service, for the duration necessary for such purposes (art. 6.1(a)-(b) ePR). Additionally, metadata may be used to meet mandatory QoS-requirements and to perform invoicing and the like (art. 6.2(a) ePR). Assuming that most of these data will qualify as personal data (see para. 2.3), there is an overlap with the GDPR. Here, the ePR is intended as a lex specialis to the GDPR, and meant to particularise its rules.

- In some respects, the particular rules provided by the ePR do not deviate materially from the GDPR-requirements. For example, the various ePR-requirements that processing is only allowed if the purpose cannot be achieved with anonymous data (art. 6.2(c) and 6.3(b) ePR) or without processing of content (art. 6.2(a) ePR) do not seem to add anything substantial to the general data minimisation principle (art. 5.1(c) GDPR). The ePR's requirement of a prior consultation for processing content data for specified purposes (art. 6.3(b) ePR), also exists under the GDPR, as processing of content

data is likely to result in a high risk to the rights and freedoms of natural persons.

3.3.2 *Impact of the ePR*

- In some respects, the ePR narrows the legal basis for processing. For example, processing of content for requested services (art. 6.3(a) ePR) or specified purposes (art. 6.3(b) ePR) may only take place on the basis of consent, whereas under the GDPR, this could be based on performance of a contract, legitimate interests, a legal obligation or even the public interest, depending on the circumstances of the case. We see no reason to rule out these alternative bases, which entail their own safeguards, including strict proportionality and subsidiarity tests.[27] Arguably, this will unduly hamper the free movement of electronic communications data and electronic communications services within the Union, as we will illustrate in our first use case (para. 7.1).

- Moreover, as we've observed in para. 2.2, the requirement to obtain consent from end-users (who can be both individuals and legal entities) is unclear and potentially problematic in practice. This further supports the argument to leave open alternative legal bases for data processing, such as legitimate interest.

- Generally the ePR's exemptions to the general ban on processing of electronic communications data are only available to ECS-providers and not to other controllers. This may also hamper innovation, as there may be other entities offering useful or even important functions in the communications chain (e.g. translation or speech-to-text tools) who may need to process electronic communications data.

4 STORAGE AND ERASURE OF ELECTRONIC COMMUNICATIONS DATA

4.1 The ePR-rules on storage and erasure of electronic communications data

Article 7 ePR contains rules on the storage and erasure of electronic communications data. As such, it particularises the general GDPR principle of storage limitation (art. 5.1(e) GDPR). Pursuant to art. 7.1 ePR, electronic communications *content* should be erased or made anonymous after receipt of such content by the intended recipients. This is without prejudice to the exemptions that an ECS-provider may rely on to process content data, as discussed in the previous chapter, i.e. if necessary for security and technical reasons (art.

[27] As explained by WP29 in its Opinion 06/2014 on the notion of legitimate interests of the data controller under art. 7 of Directive 95/46/EC, WP217.

6.1(b) ePR), to provide a specific service requested by the end-user (art. 6.3(a) ePR), or for specific purposes which cannot be fulfilled with anonymised data, with end-user consent and after consultation of the (National) Data Protection Authority (art. 6.3(b) ePR).

Articles 7.2 and 7.3 ePR contain rules on the storage and erasure of electronic communications *metadata*. Art. 7.2 requires ECS-providers to erase or anonymise all metadata when no longer needed for the purpose of the transmission of a communication. Again, this is without prejudice to the exemptions that an ECS-provider may rely on to process metadata, as discussed in the previous chapter, i.e. if necessary for security and technical reasons (art. 6.1(b) ePR), to meet mandatory QoS requirements (art. 6.2(a) ePR) or for one or more specified purposes to which the end-user has consented, which cannot be fulfilled with anonymous data (art. 6.2(c) ePR). Art. 7.3 ePR specifies that metadata may also be kept for the purpose of billing, until the end of the period during which a bill may be lawfully challenged or a payment may be pursued under national law.

STORAGE OF ELECTRONIC COMMUNICATIONS DATA (art. 7 ePR)		
Type of data	**Storage limitation**	**Other exceptions**
content	*erase after receipt by recipient and when no longer needed for other permitted processing*	*Data may be stored by end-users or third party entrusted by them*
metadata	*erase when no longer needed for the purpose of transmission and when no longer needed for other permitted processing*	*Metadata relevant to billing may be kept until end of period during which a bill may be lawfully challenged under national law*

Table 13

4.2 GDPR-rules on storage and erasure of electronic communications data (or: what if only the GDPR were to apply)

As explained in para. 2.3, it is reasonable to assume that electronic communications data should, as a general rule, be considered as personal data within the meaning of the GDPR. This is true regardless of whether the end-user is an individual or a legal entity.

As such, ECS-providers will need to observe the principle of storage limitation (art. 5.1(e) GDPR). Storage limitation means that personal data may be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which this data is being processed.

The purpose of generating and storing metadata is to achieve communication and to allow the ECS-provider to bill the service. The different legal systems of the Member States make various provisions regarding the length of time during which

actions may be initiated in contract law, so there may not be one uniform data retention period which is sufficient to allow the ECS-provider to collect payment and settle any disputes. Nonetheless it is clear the GDPR would allow ECS-providers to retain metadata for as long as necessary to achieve these purposes in each Member State, while also obliging them to delete the data as soon as this has been done.

Moreover, the GDPR has also introduced the data minimisation principle (art. 5(1)(c)). Personal data should be limited to what is necessary in relation to the purposes for which they are processed. This implies that any stored electronic communications data must be restricted to what is necessary. Only data that are adequate, relevant and not excessive in relation to the provision of the electronic communications service or for purposes of billing and interconnection payments may be processed and stored.[28]

STORAGE OF ELECTRONIC COMMUNICATIONS DATA (GDPR)		
type of data	**storage limitation**	**other relevant principles**
personal data	*no longer than necessary for the purposes for which the data are processed*	*purpose limitation* *Data minimisation* *Integrity and confidentiality*

Table 14

4.3 Analysis: overlap and impact of the ePR

4.3.1 *Overlap*

- Both the ePR and the GDPR would allow ECS-providers to store metadata for as long as necessary to collect payment and settle financial disputes and would require them to delete metadata as soon as these purposes have been fulfilled.

- Both the ePR and the GDPR require electronic communications content to be deleted immediately upon delivery, unless the data subject chooses to store these for longer, or has a third party / processor do this for them.

4.3.2 *Impact of the ePR*

- The ePR somewhat particularises the storage limitation principle by, in effect, clarifying that the purpose for which content data may be processed is transmission, and the purpose for processing metadata is invoicing. As a result, these data should be deleted once these purposes have been achieved. The ePR does not go as far as to specify a concrete storage term, so its actual added value in this respect is limited. However, full harmonisation in the form

[28] Opinion 1/2003 on the storage of traffic data for billing purposes, WP69, p. 6.

of one uniform storage term may not be achievable, as this will vary, depending on the differences in national laws pertaining to the statute of limitations for disputing or collecting invoices.

– Strictly speaking, the data retention requirements of the ePR apply to all electronic communications data, including data which does not qualify as personal data within the meaning of the GDPR. However, as set out in para. 2.3, this is unlikely to make much of a difference in practice.

5 PROTECTION OF INFORMATION STORED IN AND RELATED TO END-USERS' TERMINAL EQUIPMENT

5.1 The ePR-rules on the protection of information on end-users' terminal equipment

Art. 8 ePR aims to regulate (i) the use of the processing and storage capabilities of the terminal equipment (e.g. a website storing cookies on the device of a visitor or an app gaining access to a smartphone feature) and (ii) the collection of information from the end-users' terminal equipment (e.g. for the purpose of reading cookies) and of information emitted by terminal equipment (e.g. tracking MAC addresses from wifi-enabled devices to count the number of people in a department store). Terminal equipment is *equipment that is directly or indirectly connected to the interface of a public telecommunications network to send, process or receive information*.[29] This broad definition includes mobile devices like smartphones and tablets but also other devices with internet connectivity as diverse as desktop PCs, TV set-top boxes, and "smart home"-devices like connected speakers and thermostats.

The rationale behind art. 8 ePR is that information related to terminal equipment requires enhanced privacy protection due to the nature of the information which can be read from terminal equipment, like the content of communications, pictures, the location of individuals by accessing the device's GPS capabilities, and contact lists which may reveal details of an individual's emotional, political and social complexities.[30] According to the Commission, such enhanced privacy protection is all the more necessary since the information emitted from terminal equipment qualifies as personal data,[31] as it may enable the identification of the end-user.[32]

[29] Art. 1.1(a) Commission Directive 2008/63/EC of 20 June 2008 on competition in the markets in telecommunications terminal equipment.

[30] Recital 20 ePR.

[31] Note from the Presidency of 11 January 2018 in file no. 2017/0003 (COD), 5165/18, p. 4.

[32] Paragraph 5.2 of the Explanatory Memorandum to the ePR.

Although art. 8 has a broad scope of application, in our description and analysis below we will focus mainly on the case of cookies.

5.1.1 *General rule under ePR: data collection from terminal equipment is not allowed*

The general rule is that use of processing and storage capabilities of end-users' terminal equipment, and the collection of information from their equipment, by any party other than the end-user is prohibited. Terminal equipment information includes data about its software and hardware (the device's "fingerprint"). It is also forbidden to collect information which is emitted by terminal equipment (like the unique MAC-address of a device) to enable it to connect to another device or to network equipment. It should be noted that the general rule is not limited in its application to ECS-providers, but prohibits *anyone* from processing data from terminal equipment.

As with electronic communications data, the ePR does provide for a number of exemptions.

5.1.2 *Exemption: permitted data collection from terminal equipment by third parties (art. 8.1 and 8.2 ePR)*

The ban on the use of processing and storage capabilities of a device, and the collection of information from the device, does not apply when necessary for the sole purpose of carrying out the transmission of an electronic communication over an electronic communications network (art. 8.1(a) ePR), if the end-user has given prior consent (art. 8.1(b) ePR), if necessary for providing an information society service[33] requested by the end-user (art. 8.1(c) ePR), or if necessary for web audience measuring, provided that such measurement is carried out by the provider of the information society services requested by the end-user (art. 8.1(d) ePR).

STORING AND COLLECTING DATA FROM TERMINAL EQUIPMENT (8.1 ePR)	
exemption	**main requirement**
transmission of ECS over an EC network	*necessary for the sole purpose of transmission*
consent	*given by the end-user*
providing an information society service	*service is requested by the end-user*
web audience measuring	*measuring is carried out by the provider of the information society service requested by the end-user*

[33] The concept of information society service is now defined in Directive 2015/1535, as, in short, any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services.

Table 15

The ban on collection of information emitted by terminal equipment is lifted if the collection is done exclusively, for the time necessary, for the purpose of establishing a connection (art. 8.2(a) ePR), or if a clear and prominent notice is displayed with information on, at least, the modalities of the collection, its purpose, the person responsible for it and the other information required under the GDPR where personal data are collected, as well as any measure the end-user of the terminal equipment can take to stop or minimise the collection (8.2(b) ePR). The collection of this information emitted by terminal equipment is made conditional upon the application of appropriate technical and organisational measures in accordance with the GDPR.

COLLECTING DATA EMITTED BY TERMINAL EQUIPMENT (8.2 ePR)	
Exemption	**main requirement**
establishing a connection	*necessary and exclusively for establishment of a connection, only for the time necessary*
with clear and prominent notice	*provision of information as required by art. 13 GDPR and on measures the end-user can take to stop or minimise the collection and subject to the application of appropriate technical and organisational measures under art. 32 GDPR*

Table 16

5.1.3 *Application of art. 8.1 ePR to cookies*

For cookies, art. 8.1 ePR means that the provider of an information society service may store and read cookies from terminal equipment without the end-user's consent *only* if necessary for the sole purpose of the transmission (e.g. a 'load balancing session cookie'[34]), for providing an online service requested by the end-user (e.g. a 'user input' cookie[35]), or for ´web audience measuring´ carried out by the provider itself (and not by a third-party).

5.2 GDPR-rules for data collection from terminal equipment (or: what if only the GDPR were to apply)

Assuming that only the GDPR were to apply, would there be any restrictions on the storage and collection of data from terminal equipment? The short answer is yes.

In the recitals to the GDPR, it is expressly considered that individuals may be associated with *online identifiers* such as cookies or those provided by their devices, which may be used to create profiles to identify them.[36] This expresses a presumption that the processing of online identifiers will likely involve processing

[34] WP29's Opinion 04/2012 on Cookie Consent Exemption, WP 194, p. 8.

[35] WP29's Opinion 04/2012 on Cookie Consent Exemption, WP 194, p. 6.

[36] Recital 30 jo. art. 4(1) GDPR, see Table 2.

of personal data. Moreover, case-law of the CJEU also supports the view that unique identifiers which may be used to identify someone by legal means with additional data, will qualify as personal data within the meaning of art. 4(1) GDPR.[37]

Processing of data in connection with such unique identifiers will therefore need to comply with the requirements of the GDPR, including the principles relating to processing of personal data of art. 5 GDPR.

Looking specifically at the possible basis for the lawfulness of processing (art. 6 GDPR) for cookies, we would submit the following:

- processing of cookies and related data, which is necessary for the sole purpose of carrying the electronic transmission over an electronic communications network, can be considered as necessary for the performance of a contract where the subscriber is a natural person (art. 6.1(b) GDPR), or, in other cases, for purposes of legitimate interests by the controller or a third party (art. 6.1(f) GDPR).[38] Hence, such processing may take place without consent of the user of the device (who will qualify as a data subject within the meaning of the GDPR);

- the same is true for processing of cookies which are necessary for providing an information society service requested by the end-user, where art. 6.1(b) GDPR will apply if the end-user is the data subject who has requested the information society service, or, alternatively, the controller will be able to rely on art. 6.1(f) GDPR if the end-user is not the data subject (but, for example, the employer of the data subject using the device);

- for cookies which are necessary for web audience measuring carried out by the provider of the information society service requested by the end-user, processing of personal data can be legitimised on the basis of art. 6.1(f) GDPR, and may therefore also take place without consent;

- the same may be true for processing of personal data which takes place in the context of other cookies. Depending on the impact of this processing on the rights and interests of the data subject, this may also be based on legitimate interest, or, alternatively, on consent, provided that this meets the new, stricter, requirements of art. 7 GDPR; and

- for the purpose of solely automated decision making, including profiling, and significantly affects the data subject to the same level as a legal effect, the

[37] CJEU 19 October 2016 (Breyer), ECLI:EU:C:2016:779.

[38] We note that WP29 has expressed its opposition to open-ended exceptions along the lines of art. 6 GDPR, and in particular art. 6(f) GDPR (legitimate interest ground), WP247.

GDPR gives data subjects the right not to be subjected to automated decision-making, unless the decision is based on the data subject's explicit consent (art. 22 GDPR). Moreover, according to art. 21.2 individuals have the right to object to profiling for direct marketing purposes.

STORING AND COLLECTING DATA FROM TERMINAL EQUIPMENT (GDPR)	
purpose	**legal basis**
transmission of ECS over an EC network	*contract with data subject or legitimate interest*
consent by the end-user	*consent*
providing an information society service	*contract with data subject or legitimate interest*
web audience measuring	*legitimate interest*

Table 17

For the collection of data emitted by terminal equipment, a similar analysis may be made, as summarised in table below.

COLLECTING DATA EMITTED BY TERMINAL EQUIPMENT (GDPR)	
Exemption	**main requirement**
establishing a connection	*contract with data subject or legitimate interest*
with clear and prominent notice	*legitimate interest*

Table 18

5.3 Analysis: Overlap and impact of the ePR

5.3.1 *Overlap*

- Both the ePR and the GDPR recognise consent as a legal basis when it comes to processing of unique online identifiers (cookies, MAC addresses and related data), but also allow processing of such data without consent where this can be legitimised by the need to perform the services being requested or by legitimate technical reasons (i.e. to establish a connection).

- Neither instrument requires consent as the only possible legal basis for the processing of data if this is necessary for web audience measuring carried out by the provider of the information society service requested by the end-user, or for the processing of data emitted by terminal equipment where users have been given clear notice. Under the GDPR this is also permitted on the basis of the legitimate interest of the controller.

5.3.2 *Impact of the ePR*

- The GDPR applies only to natural persons (data subjects), whereas the ePR also applies to 'end-users concerned' which may include legal persons. Therefore, strictly speaking, legal entities may exercise the rights afforded to end-users (e.g. providing consent to place cookies). As we've observed in para. 2.2, this concept of consent from end-users is unclear and potentially problematic in practice.

- We note that in the context of art. 8 ePR, the reference to end-users could also be considered somewhat misplaced for the following reason. Provisions like art. 5, 6 and 7 ePR regulate privacy and confidentiality in the relationship between ECS-providers and those using their services. This explains the concept of end-users, who are defined by their link to the ECS and the provider of the ECS (see Table 1). Article 8, however, aims to protect terminal equipment from being accessed by any third party. Exceptions to this general ban may be open to a variety of entities (like a website publisher who uses analytics cookies or a store owner engaged in transparent wifi-tracking). The role of the ECS-provider, and their relationship to the data subject is irrelevant in this context and may even be non-existent (if someone carries a wifi-device into a store, it may be subject to wifi-tracking even if no ECS is being offered or used at that time). Therefore, in art. 8 ePR it would be more appropriate to refer to data subjects instead of end-users.

- The ePR applies to all cookies (and other data placed on or obtained from terminal equipment), irrespective of whether these can be used to identify individuals (such as the persons using the terminal equipment). The GDPR will only apply to processing of cookies and related data which can be used to identify an individual directly or indirectly. Given the low threshold this entails, and the repeated references in the GDPR to online identifiers, this difference is unlikely to be material in practice.

- Under the ePR, consent is always required for web audience measuring which is not carried out by the provider of the information society service itself, while the GDPR may allow a provider to obtain a web audience measuring service from a third party data processor, without the need to obtain consent. In that case, the provider may be able to rely on its legitimate interests. We see no justification for this particularisation in the ePR, from a perspective of the protection of fundamental rights and freedoms, while it does result in a limitation in the free movement of electronic communications data within the Union. The same could be said for other similar situations where cookies and similar technologies are being used in ways which are not detrimental to the privacy of the end-user, even if their use is not strictly necessary for carrying out the transmission or delivering the requested information society service.

– More generally, as with the rules for processing electronic communications data, the ePR narrows the legal basis for processing of data stored in and related to end-users' terminal equipment. Unless processing can be legitimised by the need to perform the services being requested or by legitimate technical reasons (i.e. to establish a connection), it may only take place on the basis of consent, whereas under the GDPR, this could be based on performance of a contract, legitimate interests, a legal obligation or even the public interest, depending on the circumstances of the case. We see no reason to rule out these alternative bases, which entail their own safeguards, including strict proportionality and subsidiarity tests. Arguably, this will unduly hamper the free movement of electronic communications data and electronic communications services within the Union, as we will illustrate in our second use case (para. 7.2).

6 OBLIGATION ON ECS-PROVIDERS TO HELP END-USERS MAKE EFFECTIVE CHOICES ABOUT PRIVACY SETTINGS

6.1 The ePR-rules on information and options for privacy settings in software permitting electronic communications

Art. 10 ePR contains rules on *software placed on the market permitting electronic communications, including the retrieval and presentation of information on the internet*. The recitals make it clear that this is intended to refer mainly to web-browsers or messaging applications.[39] We will refer to this as "ECS-software".

6.1.1 *General rule under the ePR: information and options for privacy of electronic communications software*

Art. 10 ePR aims to help end-users in making effective choices about privacy settings. It does so by imposing a general requirement for all ECS-software placed on the market to offer the option to prevent third parties from storing information on the terminal equipment of the end-user or processing information already stored on that equipment. Upon installation, the software must inform the end-user about the privacy settings options and, to continue with the installation, require the end-user actively to consent to a setting.

The rationale behind this art. 10 is specifically targeted at cookies since end-users are increasingly requested to provide consent to store tracking cookies in their terminal equipment, due to the ubiquitous use of tracking cookies and similar tracking technologies. As a result, end-users are overloaded with requests to provide consent, leading to what has been referred to as consent-fatigue. The

[39] Recital 22 ePR.

implementation of technical means in ECS-software to provide consent through transparent and user-friendly settings, is intended to address this problem.[40]

PRIVACY SETTINGS IN ECS-SOFTWARE (Art. 10 ePR)	
Art. No.	**main requirement**
10.1	*ECS-software must offer option to prevent third parties from storing or processing data on equipment*
10.2	*ECS-software must give information on privacy setting options upon installation*
10.2	*ECS-software must require end-user to consent to a setting*

Table 19

6.2 GDPR-rules for information and options for privacy of electronic communications software (or: what if only the GDPR were to apply)

Assuming that only the GDPR were to apply, would the provider of ECS-software also have a legal obligation to help end-users in making effective choices about privacy settings? The brief answer is yes.

The GDPR has codified the principle of *data protection by design*.[41] Data protection by design requires data controllers to implement appropriate technical and organisational measures which are designed to implement data-protection principles, including data minimisation, and to integrate the necessary safeguards into the processing to protect the rights of data subjects. Recital 78 of the GDPR makes it clear that this obligation is also aimed at producers of software applications which are based on the processing of personal data, who should be encouraged to take into account this principle in developing and designing their products, services and applications.

The GDPR goes even further than the ePR by also imposing the principle of *data protection by default*.[42] This implies an obligation on the part of data controllers who offer ECS-software to ensure that by default the most data protection friendly settings of applications must apply.

PRIVACY SETTINGS IN ECS-SOFTWARE (GDPR)	
requirement	**GDPR-articles**
ECS-software must offer option to prevent third parties from storing or processing data on equipment	*privacy by design (art. 25 GDPR)*
ECS-software must give information on	*transparency (art. 12, 13, 14 GDPR)*

[40] Recital 22 ePR.

[41] Art. 25.1 GDPR.

[42] Art. 25.2 GDPR.

privacy setting options upon installation	
ECS-software must require end-user to consent to a setting	*consent (art. 4.11, 7 GDPR)* *Privacy by default (art. 25 GDPR)*

Table 20

6.3 Analysis: overlap and impact of the ePR

6.3.1 *Overlap*

- Both the ePR and the GDPR clearly require ECS-software to be designed and implemented in a way which allows users to make effective choices about their privacy.

- The GDPR is stricter than the ePR, in that it requires ECS-software to be designed with the most privacy-friendly setting as the default setting, whereas the ePR merely requires ECS-software to offer the option to prevent third party access (but not necessarily by default).[43]

6.3.2 *Impact of the ePR*

- In requiring ECS-software to give end-users the right to consent to a setting, the ePR also applies to legal persons. Therefore, strictly speaking, these rights may be exercised by legal entities who are end-users, whereas consent under the GDPR only relates to individuals. This difference maybe rather theoretical, as in practice consent is likely to be given (or withheld) by the individuals who use the ECS-software, regardless of whether or not these individuals represent a legal entity.

- The GDPR applies only to providers of ECS-software who qualify as data controllers, whereas the ePR imposes a general obligation on ECS-software which must also be complied with by software producers who are not data controllers. It is possible that the entity that develops and designs ECS-software will not qualify as the data controller for any personal data that will be collected through the software. However, we believe that nowadays producers of ECS-software will in most cases (if not always) collect data through their ECS-software themselves, if only for the purpose of telemetry (collecting data on the use of the application, e.g. how often features are used, application crashes etc). As a result, most (if not all) manufacturers of ECS-software will likely qualify as data controllers, and will be bound to the GDPR.

[43] See also art. 29 Working Party Opinion 01/2017 on the Proposed Regulation for ePrivacy Regulation (2002/58/EC), WP 247, p. 14, par. 19.

7 USE CASES

7.1 Use case 1: Development of an AI support agent

This use case involves the development of an artificial intelligence-based application which is intended to take on a sales support function. The aim of the application is to deal with customer inquiries and to automatically and autonomously answer any customer queries in real time. Initially, these will be text-based queries communicated over an instant messaging platform. As technology evolves, the aim is to also support voice calls.

To build this app, a big data approach is necessary, whereby vast collections of actual customer support conversations will need to be stored and analysed for common patterns, in order to develop algorithms to deal with standard queries. These analyses are aimed both at learning how customers communicate (linguistic skills), and at identifying what the most common questions are and how these are best addressed (substantive analysis).

This approach will require collection and analysis of data which may include end-users' content data within the meaning of the ePR.

7.1.1 *Application of the ePR*

Under the ePR, the processing of content data will have to be based on either art. 6.3(a) (specific service requested by the end-user) or art. 6.3(b) (specified purposes).

A first observation to make, is that these exemptions are available only to ECS-providers. Other entities, like, for example, a software provider interested in developing this application, or an e-commerce provider who would like to use the application, cannot rely on any exemption from the general rule of confidentiality of electronic communications data.

Looking at the exemptions available to ECS-providers, the only one that might be relied on in the development phase in this example is art. 6.3(b) (specified purpose). Art. 6.3(a) (specific service) will not apply, as the analysis of communications between customer and service provider is not strictly necessary to deliver the support requested by that customer at that time. It is merely helpful to more efficiently deliver support in the future.

To be able to rely on the specified purpose exemption, the ECS-provider would need, amongst others, consent of all end-users concerned (see Table 6). This may prove problematic in this example, as individual end-users have no incentive to give consent. After all, they receive no direct benefit from the development of the application. Then there is the ambiguity around who the end-user is and how their

consent can be validly obtained. For example, when it comes to (human) customer support agents, is their consent required or that of the company they work for? Is their consent valid, given the employment context?

Aside from consent, art. 6.3(b) ePR would also require the provider to consider whether the big data analysis can be done with anonymous data, and also to consult the supervisory authority beforehand (see Table 6). In this use case, anonymisation may not always be the solution, where analysing voice communications cannot be done with anonymous data as voice is inherently personally identifiable.

7.1.2 *Application of the GDPR*

The content data that will be analysed as part of the development process, will contain personal data. As a consequence, this processing will have to comply with the GDPR (see, in particular, Table 12).

It is likely that the development of the application may be based on the developer's (or the app's future users') legitimate interests, which outweigh the privacy interests of the data subjects, providing that suitable safeguards will have been implemented. These safeguards may include enhanced transparency on this issue, an opt-out and the application of anonymisation techniques.

The developer will have to consider the data minimisation principle, which will require him to address if the processing of personal data will be limited to what is necessary in the relation to the purposes for which they are processed. This will ultimately centre on the question of whether the same purpose cannot also be achieved without the processing or by processing aggregated data. Under the GDPR, the developer will also have to perform a data protection impact assessment (art. 35 GDPR) prior to the development process, if the analysis poses a high risk to the data subject and cannot be based on anonymous data. If it is not able to mitigate the high risks which its plans pose, it will have to consult the supervisory authority prior to its processing (art. 36 GDPR). These steps are more or less the same as those required under art. 6.3(b) (specified purposes).

7.1.3 *Conclusion*

In short, the outcome under the ePR would be quite different from the outcome under the existing rules of the GDPR, although there are also similarities:

- under the ePR, only an ECS-provider might be able to collect and analyse actual customer support conversations, and then only with end-user consent. This is likely to present a substantial hurdle to the big data approach; and

- under the GDPR, a data controller (which could also include the developer of the application) may be able to rely on legitimate interest, subject to strict safeguards; and

- the outcome is very similar when it comes to data minimisation (the need to anonymise where possible) and prior consultation of the supervisory authority.

7.2 Use case 2: Use of device fingerprinting for fraud prevention

Our next use case concerns the use of device fingerprinting technology for fraud prevention purposes.

A large online trading platform, which allows non-professional traders to sell products to consumers, applies a variety of fraud prevention tools to protect both its traders and their customers. One technology it wants to implement is a form of device fingerprinting. It will obtain information like the type of device (hardware/OS version), language settings used, IP-address and connection type (e.g. use of proxy-servers), for both traders and buyers, and use this as a factor to determine a risk profile. If the overall risk profile of a trader or buyer exceeds a certain level, the trading platform may act on this information to protect its own interests and those of the users of its platform, by sending a warning, preventing a transaction and/or blocking a user.

7.2.1 *Application of the ePR*

Under the ePR, this particular form of device fingerprinting will have to be based on art. 8.1(b) (prior consent of the end-user). Other exemptions (see Table 15) do not apply:

- the processing of this device-data is not necessary for the sole purpose of carrying out the transmission (art. 8.1(a));

- nor is it, strictly speaking, necessary for the provision of an information society service requested by the end-user (art. 8.1(c));

- or related to any form of web audience measuring (art. 8.1(d)).

Consent of the end-user is problematic in the context of fraud prevention, as end-users with fraudulent intent are unlikely to provide it.

7.2.2 *Application of the GDPR*

Processing of online identifiers provided by the device of a user is likely to qualify as processing of personal data, especially if this is collected together with additional information like an IP-address, and is used for (risk) profiling purposes.

As a consequence, this processing will have to comply with the GDPR (see, in particular, Table 17 and Table 18).

It is likely that this particular use of device finger printing may be based on the platform (or its users') legitimate interests, which outweigh the privacy interests of the data subjects, providing that suitable safeguards will have been implemented. These safeguards may include enhanced transparency on this issue.

The platform provider will have to consider the data minimisation principle, which will require him to address if the processing of personal data will be limited to what is necessary in relation to fraud prevention. This will also involve the question of whether the risk of fraud cannot be reduced just as effectively by alternative means without this particular form of device fingerprinting. Moreover, the provider will of course also need to comply with all other requirements of the GDPR (including those set out in Table 7).

7.2.3 *Conclusion*

Again, the outcome under the ePR would be quite different from the outcome under the existing rules of the GDPR:

- under the ePR, this particular form of device fingerprinting would only be allowed with end-user consent. This would most likely render this solution useless for fraud prevention purpose; and.

- under the GDPR, a data controller may be able to rely on legitimate consent, subject to strict safeguards.

8 GENERAL CONCLUSIONS

Based on the findings presented in this study, we believe the following general conclusions are warranted:

- the area of overlap between the ePR and the GDPR is substantial. The extent to which the ePR intends to particularise the rules of the GDPR is much larger than the extent to which it complements the GDPR (see Figure 1);

- where the ePR intends to add to or deviate from the GDPR, it does not actually always do so. For example:

    - the general GDPR requirements to secure the confidentiality of personal data already provide substantial protection against unlawful interference with electronic communications (art. 5 ePR);

- the requirement under art. 6 ePR to check that the purpose cannot be fulfilled by processing anonymous data, also follows from the GDPR's data minimisation principle which implies minimisation of personal data but does not extend to anonymous data which are outside of the GDPR's scope;
- the ePR requirements in art. 7 ePR to delete metadata if no longer necessary to collect payments and settle disputes, or to delete content immediately upon delivery (unless the data subject chooses to store this longer), do not add anything meaningful to the general data retention requirements of the GDPR; and
- the requirement of art. 10 ePR for ECS-software to help end-users make effective privacy choices, adds little to the GDPR's privacy-by-design principle.

– In other instances where the ePR aims to particularise the general rules, it is unclear what the added value is, either in terms of enhancing data protection rights, or supporting the free movement of data and services. In particular, there is an overreliance on consent, which would exclude other legal bases permitted under the GDPR, like the need to process data for the purposes of 'legitimate interest'. For example:

  - content may only be processed, outside the scope of delivering the ECS, for specifically requested services or for specified purposes (art. 6.3 ePR). In both cases, such processing may only be undertaken by the ECS-provider (and not any third party), and requires the consent of some or all end-users (see Table 6). This significantly narrows the possibilities that the GDPR allows for, i.e., processing without consent, by any controller with a sufficient legitimate interest, subject to the safeguards and requirements that the GDPR entails, as our first use case illustrates (see para. 7.1); and
  - the ePR's rules on using terminal equipment to store information, or collecting information from such equipment (art. 8 ePR), only recognise limited exceptions to the requirement of consent (i.e. necessary for the sole purpose of transmission, to provide a requested information society service, or for web audience measuring carried out by the provider). This is an unduly restricted approach, which would disallow other legitimate use cases (see, for example, para. 7.2).

– To the extent that the ePR extends the rules of the GDPR, its added value may also be marginal or not obvious, for the following reasons:

  - the ePR may also apply to communications data of legal entities (whereas the GDPR does not). However, in most cases these data will also relate to natural persons, and therefore fall within the scope of the GDPR (see para. 2.2 and 2.3);

- the ePR imposes rules on the use of information stored in and related to end-users' terminal equipment, regardless whether such information qualifies as personal data. However, this extension of the rules is unlikely to be material in practice, as we believe in practice such terminal equipment data will almost always be considered personal data (see para. 2.3);
- to the extent that communications data or data relating to terminal equipment do not qualify as personal data (e.g. M2M applications in a purely industrial context), one may question the added value of applying privacy principles to such data, also in light of alternative existing protections for such data, arising from, for example, the Convention on Cybercrime and the Directive on trade secrets; and
- it is unclear how the concept of 'consent from end-users' should be interpreted and applied, when the end-user is a legal entity (para. 2.2).