HÄRTING

# Study on the Impact of the Proposed ePrivacy Regulation

## 19 October 2017

FOR **Centre for Information Policy Leadership**
30 St Mary Axe
London, EC3A 8EP

FROM **HÄRTING Rechtsanwälte PartGmbB**
Prof. Niko Härting
Chausseestraße 13
10115 Berlin

## Executive Summary

### General effects of the ePR

1. The ePR and the GDPR **overlap** substantially. In many cases, the ePR rules deviate from the GDPR. This would be bound to lead to **legal uncertainty** and will be harmful to European businesses.
2. With the prohibition of "processing" communications data, the ePR would be a **serious obstacle to digital innovations** in Europe and to the development of new beneficial services based on data use and machine learning. The prohibition of "processing" would constitute a substantial **setback to the European digital economy**.
3. The ePR would **impede the free flow of data** in Europe. Abundant consent requirements would lead to **red tape** and **tick boxes**.
4. Abundant tick boxes are likely to **irritate consumers.** This will impact their online experience negatively.
5. The ePR mainly focusses on protecting consumers' privacy by **consent requirements**. It would therefore be up to consumers to protect their privacy themselves (by giving or refusing consent). Shifting the responsibility from businesses to individual consumers **cannot be regarded as an enhancement of the protection of privacy**.

### Art. 5 ePR - Confidentiality of electronic communications data

1. The **interception and surveillance** of communication constitute **severe infringements of privacy**. The prohibition of interception and surveillance is, therefore, appropriate.
2. Although **data security** is a major issue in digital communications, the **ePR does not contain provisions on security**.
3. Art. 5 ePR introduces a **new prohibition of** the **"processing"** of communications data. However**,** it is exactly the "processing" of communications data that that the customer pays for (as opposed to "interception" or "surveillance").
4. Without the "processing" of electronic data, there is no electronic communication. **Electronic communication** is a **fundamental right**. It is, therefore, **wrong to prohibit** the processing of electronic communications data and to treat such processing as a severe risk to privacy similar to the interception and surveillance of messages.

**Art. 6 ePR - Permitted processing of electronic communications data**

1. Art. 6 ePR introduces **new consent requirements** for the processing of **content** and **metadata** by service providers.
2. The strict consent requirements **contradict Art. 6 GDPR**. When the customer pays the service provider for "processing" content and/or metadata, consent is not necessary according to the GDPR, and it is unclear why there should be a consent requirement in the ePR.
3. As far as **metadata** are concerned, it is unclear why IP addresses and other "online identifiers" **clearly covered by the GDPR** need to be regulated in the ePR as well-
4. Art. 6 ePR does not work for **machine-to-machine communication**, for **wearables**, **connected cars** and the **Internet of Things (IoT)**. In machine-to-machine-communication, **raw data** are transmitted that do neither qualify as "content" nor as metadata.
5. **Art. 6 (3) ePR** is clearly **excessive** as it demands the **spammer's consent** for the use of a spam filter.

**Art. 7 ePR - Storage and erasure of electronic communications data**

1. When a customers uses a digital communications services (e.g. email, messenger), he will expect his messages to be stored by the provider. Moreover, he will expect to be in control when it comes to the erasure of messages. Therefore, the provider's **duty to erase content** is **against the user's interests** and contrary to his expectations.
2. As far as **personal data are** concerned, the service provider's duties to erase are covered (and limited) by Art. 17 and 20 GDPR. It is unclear why additional provisions should be necessary in the ePR.

**Art. 8 ePR - Protection of information stored in and related to end-users' terminal equipment**

1. As "**online identifiers**" cookies are **covered by the GDPR**. It is unclear why additional provisions should be necessary in the ePR.
2. Art. 8 ePR **contradicts Art. 6 GDPR**. According to Art. 6 GDPR both the **performance of a contract** and **legitimate interests** pursued by the controller may be reasons for the lawful processing of cookies whereas there are no such exceptions in the ePR.
3. Browser settings are, at the same time, regarded as "**user-friendly**", making it easier for the user to give consent to cookies, and as "**gatekeepers**", preventing cookies from being stored. This is clearly **contradictory.**
4. **Web analytics tools** are, on the one hand, recognized as "legitimate and useful". On the other hand, hardly any analytics tool will be covered by the exception from the consent requirement as the exception is only applicable when a website operator is using his own analytics tool. Again, this is **contradictory**.

5. To be on the safe side, operator of websites will need to ask users individually for their consent if he or she wants to set cookies. This will lead to **recurring cookie banners** and an **overload of requests.**
6. Fingerprinting falls under the "cookie provision" of Art. 8 ePR and requires **consent**. For the time being, it does not appear to be realistic to expect that there will be **browser settings** on the market soon that meet the requirements of consent for fingerprinting. There are presently **no standards** for such settings on the market, and the standards that can be found the **ePR** focus exclusively on cookies and **neglect fingerprinting and other non-cookie tracking technologies**.
7. **WI-FI and Bluetooth** tracking are prohibited by **Art. 8 (2) ePR**. Art. 8 (2) ePR **lacks** a **consent exception**. This is not in line with the intention of making consent the "central legal ground" of the ePR.
8. Both WI-FI and Bluetooth tracking are covered by the provisions of the **GDPR**. "Identification numbers" are explicitly mentioned in the list of (possibly) personal data in Art. 4 GDPR. The comprehensive rules on the processing of such data in Art. 6 GDPR are **far more balanced and risk-orientated** than Art. 8 (2) ePR.
9. While browser settings are a central element in the proposed rules on cookies and even though every device has an "on/off" button both for WI-FI and for Bluetooth signals, the **device settings** do not play any role in Art. 8 (2) ePR.
10. The obligation to display "**prominent notices**" limits the lawfulness of WI-FI and Bluetooth tracking to tools that monitor a **building** or a **pre-defined area**. Important fields of use of the technology like **traffic monitoring** and **Bluetooth networks** do not allow the definition of a geographical area of use and the display of "prominent notices". Art. 8 ePR, therefore, **severely impedes** the **further development of offline tracking tools** although Recital 25 ePR concedes that there are areas of use void of high privacy risks.
11. It is worth noting that intrusions on privacy resulting from the "sending of commercial messages to end-users" are covered by **Art. 16 ePR** ("Unsolicited communications"). It is unclear why the opt-in rules provisions of Art. 16 ePR should not be sufficient for the protection of privacy against offline tracking when the purpose of such tracking is **targeted advertising**.

**Art. 9 ePR – Consent**

1. The over reliance on consent is based on **false assumptions** when it comes to **legal persons**. The ePR aims at protecting privacy and at extending such protection to legal persons. However, it is unclear **whose consent** is relevant.
2. An efficient protection of privacy would mean that the **user of a device** is the person who needs to give consent. This, however, will always be a natural person whose privacy is already **protected by the GDPR**. Alternatively, it can be the **legal representative** of the legal person (company or government agency) who needs to be asked for consent. This can **hardly be regarded as** an **adequate** means of protecting the employees' privacy.

**Art. 10 ePR - Information and options for privacy settings to be provided**

1. While the main focus of Art. 10 ePR lies on **web browsers**, there are various other software products and applications that Art. 10 ePR covers. This is mainly true for **apps**. Many apps "permit electronic communication".
2. Art. 10 ePR obliges **app providers** to enable users to prevent the storing of "information". However, exactly such **storage** will often be a **fundamental function** of the app. There is no reason why the provider of a messenger app should be obliged to enable his or her customers to prevent the storing of messages, pictures and voice files on their smartphones although the receipt and (temporary) storage of content is the main purpose of the app.
3. In Art. 10 (1) ePR, The term "**third parties**" is **misleading** as it is unclear whether the duty to prevent the storage of information means, generally, the storage of **all cookies** by ("third") persons who are neither the user nor the browser provider ("reject all cookies") or just the storage of "**third person cookies**" ("reject third party cookies").

**Art. 11 ePR - Restrictions**

1. Art. 11 ePR **lowers the threshold** for EU or member state laws that permit wiretapping or other means of surveillance, including **data retention**, and ignores the restrictions on data retention and bulk collection resulting from the principles that the **ECJ** set up. According to the ECJ, no "general and indiscriminate retention of data traffic and location data" is permissible irrespective of the purposes of such retention.
2. As providers of messenger, webmail, VoIP and other **"over the top (OTT)" services** are now included in the scope of the ePD, Art. 11 ePR **silently introduces new obligations** for many providers to co-operate with law enforcement agencies. This clearly contradicts the chief goal of the ePR, which is to protect the privacy of EU citizens.

# 1 Overview

On January 10th, 2017, the European Commission published the draft of a new European ePrivacy Regulation (ePR)[1]. It is the aim of the Commission to replace the existing ePrivacy Directive (ePD) by the new regulation when the General Data Protection Regulation (GDPR) comes into effect on May 25th, 2018.

The main focus of both the GDPR and the ePR/ePD is the protection of European citizens' privacy. Since the 1990s, there have been EU provisions on data protection and privacy. Data protection in the **telecommunications sector** has always been dealt with as a separate issue and not as a part of privacy regulation in general.

Parallel to the EU Data Protection Directive of 1995 (DPD)[2], the EU Telecommunication Privacy Directive of 1997 (TPD)[3] was negotiated and enacted[4]. Soon, it became clear that the TPD was too focussed on traditional fixed telephony. The TPD was therefore repealed and replaced by the **ePrivacy Directive (ePD)** of 2002[5]. The new Directive aimed at incorporating the principle of technology neutrality into the regulation of data protection in the telecommunications sector[6].

Now that the DPD has been replaced by the General Data Protection Regulation (GDPR)[7], the European Commission intends to replace the ePD by a new ePrivacy Regulation (ePR)[8].

Similar to the ePD, the draft ePR is a "**mixed bag**" and deals with diverse issues ranging from the confidentiality of communication (Art. 5 ePR) to incoming call blocking (Art. 12 ePD) and marketing communications (Art. 16 ePR)[9].

There are numerous references in the ePR to the **GDPR**. According to Art. 1 (3) ePR, the provisions of the ePR are to "particularise and complement" the GDPR ("lex specialis"[10]). At the same time, the ePR aims to protect "fundamental rights and freedoms of natural and legal persons in the provision and use of electronic communications services" (Art. 1 (1) ePR) while ensuring "free movement of electronic communications data and electronic communications services" in the EU (Art. 1 (2) ePR).

---

[1] Proposal for an ePrivacy Regulation, Jan 10th, 2017, https://ec.europa.eu/digital-single-market/en/proposal-eprivacy-regulation.
[2] Directive 95/46/EC.
[3] Directive 97/66/EC.
[4] Costa, Consent in European Data Protection Law, 2013, p. 261/262.
[5] Directive 2002/58/EC.
[6] Costa, Consent in European Data Protection Law, 2013, p. 263/264.
[7] Regulation (EU) 2016/679-
[8] COM(2017) 10 final.
[9] See German Bar Association, Position Paper on the ePR draft, p. 9 et seq., https://anwaltverein.de/de/newsroom/sn-29-17-stellungnahme-zur-eprivacy-vo.
[10] COM(2017) 10 final, p. 2

While the GDPR only protects the rights and freedoms of natural persons,[11] there is no distinction between **natural and legal persons** in the ePR. The ePR explicitly aims to ensure that provisions of the GDPR "apply to end-users who are legal persons" (Recital 3 ePD). While the ePR does not intend to lower the level of protection enjoyed by natural persons under the GDPR (Recital 5 ePD), it is unclear to what extent the ePR may impose restrictions on the **free movement of data** that go beyond the restrictions resulting from the GDPR.

This study focusses on the proposed new "**cookie provisions**" (Art. 8, 9 and 10 ePR) and on the proposed "**interference provisions**" (Art. 5, 6 and 7 ePR) including the "**wiretapping provisions**" of Art. 11 ePR. In particular, this study explores the following issues:

- **Practicability**: Are the proposed provisions coherent and does their application on standard business models lead to reasonable results?
- **Overlap**: Are the proposed provisions in line with the provisions of the GDPR? Are there contradictions?
- **Freedom of Communication:** Do the proposed provisions foster free communication data in Europe or do they – unintendedly - impose obstacles on communication?
- **User-Friendliness**: Do the proposed provisions meet the expectations of reasonable users?

[11] Art. 2 (1) and Art. 4 (1) GDPR.

# 2 Confidentiality of electronic communication ("interference regulation")

## 2.1 Confidentiality (Art. 5 ePR)

Art. 5 ePR protects the confidentiality of electronic communications. According to Art. 5 ePR, any „interference" with and "surveillance" of electronic communications data is prohibited, except when permitted by the ePD. It is not just "**interference**" and "**surveillance**" that is prohibited by Art. 5 ePR but also the mere "**processing**" of electronic communications data:

> "*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.*"

According to **Art. 5 (1) ePD**, the confidentiality of communications was also protected, and the "interception" or "surveillance" of communications was prohibited. It is, however, worth noting that the "**processing**" of communications data was **not prohibited**[12].

From the perspective of a service provider and his customer, the introduction of a prohibition of processing communications data makes a **significant difference**. Whatever the service may be, the processing of communications data will always be one of the **core activities of the service provider**. In many cases, it is exactly the "processing" of data that that the customer pays for (as opposed to "interception" or "surveillance" that the customer may want to be protected from).

Just as Art. 5 ePD, Art. 5 ePR protects **personal as well as non-personal information**. As far as personal information is concerned, there is no distinction between **natural and legal persons**.

**Confidentiality** of communication is also protected by the GDPR. **Art. 5 (1) (f) GDPR** explicitly mentions "confidentiality" as one of the **principles** of the GDPR. The GDPR, however, only protects confidentiality as far as personal data are concerned and only when such data relates to a natural (as opposed to a legal) person.[13] It is worth noting that the principle of "confidentiality" has been **newly introduced** in the GDPR. It was not included in the general principles of the DPD (Art. 6 DPD).

It is also worth noting that there is an inherent link between privacy and the confidentiality of communication. Communication is always interaction between two human beings. When using electronic services, they will normally assume their interaction to be confidential, and they

---

[12] German Bar Association, Position Paper on the ePR draft, p. 17, https://anwaltverein.de/de/newsroom/sn-29-17-stellungnahme-zur-eprivacy-vo.

[13] *Heberlein* in Ehmann/Selmayr (ed.), GDPR, 1. Edt. 2017, Art. 5 (1) p. 271.

will rely on the confidentiality. Whether the content of communication contains personal data or not, the protection of confidentiality always serves to protect the privacy of the **interaction of human beings** ("natural persons").

The **interception and surveillance** of communication constitute **severe infringements of privacy**. It is, therefore, evident that both the government and private entities must not be allowed to intercept or surveil communication unless there is a good reason justifying such an infringement. The prohibition of interception and surveillance in Art. 5 ePD and Art. 5 ePR makes sense.

The same does not apply to the mere processing of communication data. **Communication** is an **essential freedom** of citizens. Without communication, there is no human/social interaction. The freedom of expression and information is protected by **Art. 11 ECFR**, and any ban on communication would be incompatible with human dignity (Art. 1 ECFR).

In the digital age, the use of electronic services is essential for human communication and interaction. Without the processing of electronic data, there is no electronic communication. It is, therefore, wrong to prohibit the processing of electronic communications data and to treat such processing as a severe risk to privacy on the same level as the interception and surveillance of messages.

The prohibition of the processing of electronic communications protects the end-users against electronic communication. This does not correspond to the main goal of the ePR to protect fundamental rights[14].

### 2.2 Permitted Processing (Art. 6 ePR)

Art. 6 ePR defines the conditions under which the processing of communications data is lawful by distinguishing between

- electronic communications **networks** and electronic communications **services** and between
- electronic communications **content** and electronic communications **metadata**.

**Art. 6 (1) ePR** applies to

- services and networks and to
- content and metadata.

[14] See German Bar Association, Position Paper on the ePR draft, p. 18, https://anwaltverein.de/de/newsroom/sn-29-17-stellungnahme-zur-eprivacy-vo.

**Art. 6 (2) ePR** applies to

- services and
- metadata.

**Art. 6 (3) ePR** applies to

- services and
- content.

As far as **networks** are concerned, only Art. 6 (1) ePR applies. Providers of electronic communication networks may therefore process content and metadata if processing is necessary for the transmission of communication (Art. 6 (1) (a) ePR) or when processing is necessary for security or technical reasons (Art. 6 (2) ePR). **Consent** is **not required**.

As far as **services** are concerned, Art. 6 (2) and (3) ePR rely heavily on **consent**. For the processing of communications **content**, consent is always necessary (Art. 6 (3) ePR). As far as metadata are concerned, consent is necessary unless the processing of **metadata** is necessary for billing or for the detection or prevention of fraud or abuse or for meeting mandatory service requirements (Art. 6 (2) ePR).

As the **ePD** did not prohibit the processing of **content**, there are no provisions in the ePD on permitted processing. In particular, there are **no consent requirements**.

According to Art. 6 (1) **ePD**, **traffic data** could be processed and stored but needed to be erased or made anonymous when it was no longer needed. Further processing for billing purposes was permitted (Art. 6 (2) ePD). Processing for marketing purposes required consent (Art. 6 (3) ePD).

Traffic data was defined as "data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing thereof" (Art. 2 (b) ePD) whereas the (**significantly broader**) term "**metadata**" is now in **Art. 4 (3) (c) ePR** defined as

> *"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".*

Compared to the ePD,

- there are **new consent requirements** for the processing of **content** by service providers;

- there are **new consent requirements** for the processing of "**metadata**" (as opposed to mere "traffic data")[15].

### 2.3 Storage and erasure (Art. 7 ePR)

According to Art. 7 (1) ePR, service providers must erase communications **content** or make the content anonymous after receipt by the intended recipient(s). The same applies to **metadata** when it is no longer needed for the purpose of a communication (Art. 7 (2) ePR). As far as metadata are concerned that is processed for billing purposes, such metadata may be kept until the end of the period during which a bill may lawfully be challenged or a payment may be pursued in accordance with national law (Art. 7 (3) ePR).

There were provisions similar to Art. 7 ePR in Art. 6 (1) and (2) ePD for "traffic data". It is, however, unclear what significance Art. 7 ePR can have when the processing of communications data is only permitted under the conditions of Art. 6 ePR:

- As far as **personal data are** concerned, the service provider must erase such data when data are no longer necessary in relation to the purposes for which they were collected or otherwise processed according to **Art. 17 (1) (a) GDPR**.[16]
- As far as **other data** are concerned, further processing is illegal unless the conditions of Art. 6 ePR are met. It would suffice to refer to Art. 17 GDPR in case non-personal data are stored illegally ("Art. 17 GDPR applies accordingly").

### 2.4 Case Studies

#### 2.4.1 Wearables: "Fitbit Surge"

Wearables are devices worn on the body as accessories or as part of materials used in clothing. They can usually connect to other devices like smartphones, tablets or PCs. A major feature of the **wearable technology** is its ability to connect to the internet and to exchange data.

Typical functions of wearables are:

- GPS tracking;
- pedometer;
- measuring the heart rate and caloric burn.

[15] See German Bar Association, Position Paper on the ePR draft, p. 19, https://anwaltverein.de/de/newsroom/sn-29-17-stellungnahme-zur-eprivacy-vo.
[16] See also *Herbst* in Kühling/Buchner(ed.), GDPR, 1. Edt. 2017, Art. 17 p. 412.

**Fitbit Surge** is a wristband containing a device that collects data like the number of steps and the heart rate as well as location data (GPS signals, device sensors, WIFI access points and cell tower IDs)[17]. The data are transferred from the device to Fitbit servers whenever the device is synchronized through a Fitbit app or Fitbit software. **Transmission data** will be recorded during the synchronization. These include the date and time of the synchronization, the battery or battery level of the device, and the IP address used during synchronization.[18]

#### 2.4.1.1 Electronic Communication Service

In order to determine if Fitbit Surge falls in the scope of the ePR, it is necessary to examine whether it can be classified as an "electronic communication service" within the meaning of the ePR.

Article 4 (1) (b) ePR refers, for the definition of "electronic communication services", to the EECC. Article 2 (4) EECC defines an "electronic communications service" as

> "[…] *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.*"

The Fitbit Surge device is connected via Bluetooth to a smartphone or to a PC. Fitbit Surge records data and synchronizes and transfers data to Fitbit servers. The transmission of the signals can be classified as a **machine-to-machine service**. The operating principles of the "Fitbit Surge" comply with Art. 4 (1) (b) ePR and fall under the definition of "electronic communication services".

**Recital 12 ePR** explicitly mentions that the ePrivacy Regulation should apply to machine-to-machine communication:

> "***Connected devices*** *and machines increasingly communicate with each other by using electronic communications networks (Internet of Things).* […]. *In order to ensure full protection of the rights to privacy and confidentiality of communications* […] *it is necessary to clarify that* ***this Regulation should apply to the transmission of machine-to-machine communications****. Therefore, the principle of confidentiality enshrined in this Regulation should also apply to the transmission of machine-to-machine communications.* […]."

[17] See https://www.fitbit.com/legal/privacy.
[18] See https://www.fitbit.com/legal/privacy-policy.

#### 2.4.1.2 Content and Metadata

For the legal assessment, it is necessary to determine whether the transmitted data fall under the definition of "electronic communication data" and what kind of data (content or metadata) the "Fitbit Surge" device is processing.

Pursuant to article 4 (3) (a) ePR, "electronic communication data" means

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

The ePR defines "electronic communications content" in article 4 (3) (b) ePR as

> "*the content exchanged by means of electronic communications services, such as text, voice, videos, images, and sound*".

The definition contains **examples** that are **not exhaustive**. The exact meaning of "content" is not clear for machine-to-machine services. Typically, there is no transmission of data that can be genuinely classified as "*text, voice, videos, images, and sound*".

The Fitbit Surge device simply collects **raw data**. The data are processed on Fitbit servers, and it is only on the servers that content is produced, e. g. **statistics** about the number of steps per day the user has walked or about the heart rate and calory burn during a run.

For lack of electronic communications content (Art. 4 (3) (b) ePR), the data transmitted by the Fitbit Surge device to Fitbit Servers might still qualify as metadata within the definition of Art. 4 (3) (c) ePR. The definition, however, only encompasses data processed "for the purposes of transmitting, distributing or exchanging electronic communications content". When there is no transmission of content, there can, logically, be no (meta)data processed "**for the purpose of"** such a transmission.

#### 2.4.1.3 Results

The results of the analysis are confusing:

- Recital 12 ePR: It is clearly the aim of the ePR to include **machine-to-machine communication** in its scope.
- Art. 5 ePR: The principle of confidentiality only applies to electronic communications data, meaning either content or metadata (Art. 4 (3) (a) ePR).
- Content: In machine-to-machine-communication, **raw data** are transmitted that do not qualify as "content" (Art. 4 (3) (b) ePR).
- Metadata: By definition, there can be no transmission of metadata when there is **no content** that is transmitted. Raw data does not, as such, qualify as metadata within the meaning of the ePR (Art. 4 (3) (c) ePR).

- **Consent requirements**: There are different sets of consent requirements in Art. 6 (2) and (3) ePR for content and metadata. It is **unclear** if and which of there requirements apply to mere raw data.
- **Erasure requirements:** There are different erasure requirements for content and metadata in Art. 7 (1) and (2) ePR. Again, it is **unclear** if and which of there requirements apply to mere raw data.
- **GDPR:** There can be no doubt that data collected by a wearable is personal (Art. 4 (1) GDPR). This is true for the raw data collected by the device and also for the information ("content") gained by processing the data on a (Fitbit) server. The collection and processing of such data or information will, in many cases, be covered by Art. 6 (1) (b) GDPR as, when there is a contract between the user and the wearable provider, the collection and processing of data will be necessary for the **performance of the contract**. Under which aspects additional protection (by consent and erasure requirements, Art. 6 and 7 ePR) should be necessary or justified, is entirely unclear.

The results of the analysis do not only apply to wearables but to the **Internet of Things (IoT)** in general,[19] in particular to **connected cars**. The vast amounts of data collected by cars and transmitted to servers for processing[20] exclusively consist of raw data. Therefore, it is unclear if and to what extent Art. 6 and 7 ePR apply. Moreover, the raw data as well as the information ("content") gained by processing the data, will, in many cases be personal and, therefore, covered by the **GDPR** (Art. 4 (1) (a) GDPR). The confidentiality of personal data is explicitly protected by Art. 5 (1) (f) GDPR. It is **unclear** why there should be a need for additional protection by **additional consent requirements**.

### 2.4.2 Spam Filters: "Gmail"

Email providers use filters to detect **spam** and **malware** in order to enable an efficient use of the mail service. Far more than half of email communication is spam and malware which can harm the end-user[21]. There are **billions of spam mails**, so without filtering messages the use of email services would be seriously burdened.

Email providers use several spam detection techniques which are based on scanning the content of mails. Often, a "**black list**" is used of known spammers collected by internet service

[19] See Klar/Buchner in Kühling/Buchner (ed.), GDPR, 1. Edt. 2017, Art. 4 (1) p. 127.
[20] See FIA reveals what data is being tracked and how the public reacts to connected cars, Nov. 25th, 2015, http://www.fia.com/news/fia-reveals-what-data-being-tracked-and-how-public-reacts-connected-cars
[21] See Global spam volume as percentage of total e-mail traffic from January 2014 to March 2017, by month, https://www.statista.com/statistics/420391/spam-email-traffic-share/

providers (ISPs), email providers and server administrators[22]. In addition, there are various **authorization procedures** that can be used to distinguish false mail addresses from real ones.

Depending on the filter and setting, emails containing a feature from the blacklist are either deleted or marked as spam and moved to a specific folder. In obvious cases of spam and malware, the message is not even delivered

Email providers also often work with **"white lists"**. The provider maintains a list of sender addresses to ensure that the incoming messages always land in the inbox. Furthermore, most mail providers have a so-called **training mode**[23]. The filter lists (black lists and white lists) can be adjusted by the user by marking individual emails as "spam/malware" or "safe" to improve the efficiency of the spam filter.

Filters scan the incoming communication the following information:

- **IP address:** The webmail provider scans the IP address of the sender. If a mail comes from an IP address which is known to send spam or malware, it is sorted out.
- **Sender address:** The email provider scans the sender address to decide whether it is a spammer. For this purpose, a comparison with senders with which the recipient has already been communicated is made.
- **Content:** The webmail provider scans the content of an email and searches in the subject line and the message for specific keywords.

**Gmail** enables users to send and receive emails via electronic communications networks. The sender usually determines the recipient(s), and the exchange takes place between a finite number. Thus, Gmail qualifies as an “interpersonal communications service” and therefore as an “electronic communication services” pursuant to Art. 4 (1) (b) ePR/Art. 4 (2) and (5) EECC.

#### 2.4.2.1 Confidentiality (Art. 5 ePR)

According to Art. 5 ePR, the **scanning of electronic communications** data by persons other than the end-users is prohibited unless the end-users have given their consent or the interference is permitted by the ePR.

Gmail scans the content and metadata for unwanted messages and malware. The IP address and the mail address of the sender as well as the content and the attachment of the email are scanned and matched with a blacklist. Depending on the filter and setting, emails containing a

[22] Gillin, The Art and Science of How Spam Filters Work, SecurityIntelligence, Nov. 2nd, 2016, https://securityintelligence.com/the-art-and-science-of-how-spam-filters-work/.
[23] Gillin, The Art and Science of How Spam Filters Work, SecurityIntelligence, Nov. 2nd, 2016, https://securityintelligence.com/the-art-and-science-of-how-spam-filters-work/.

feature from the blacklist are either deleted or marked as spam and moved to a specific spam folder.

In **Recital 19 ePR**, spam filters are seen as a threat to communication rather than as a means to foster and enable communication:

> *"For example, providers may offer services that entail the scanning of emails to remove certain pre-defined material. Given the sensitivity of the content of communications, this Regulation sets forth a **presumption that the processing of such content data will result in high risks to the rights and freedoms of natural persons**. When processing such type of data, the provider of the electronic communications service should always consult the supervisory authority prior to the processing. Such consultation should be in accordance with Article 36 (2) and (3) of Regulation (EU) 2016/679."*

With Recital 19 ePR explicitly regarding spam and malware filters as **risks to confidentiality**, it is no surprise that such filters fall under the prohibition of Art. 5 ePR.

#### 2.4.2.2 Consent Requirements (Art. 6 ePR)

Art. 6 ePD distinguishes between

- electronic communication **networks** and electronic communication **services** and between
- electronic communications **content** and electronic communications **metadata**.

According to Art. 2 (1) EECC (Art. 4 (1) (b) ePR), "electronic communication **networks**" 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".*

Pursuant to Art. 2 (4) EECC, "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".*

According to Art. 2 (5) EECC, "**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".*

If a user sends emails via Gmail, both content and metadata are sent and arrive in the recipient's inbox. Thus, the service is a service that enables **interactive exchange of information** via electronic communication. It is, therefore, interpersonal (Art. 2 (5) EECC), and it is an electronic communication service (Art. 2 (4) EECC) as opposed to electronic communication networks (Art. 2 (1) EECC).

For services, all the three paragraphs of Art. 6 ePR apply. As far as content is concerned, Art. 6 (1) and (3) ePR are applicable. As far as metadata are concerned, Art. 6 (1) and (2) apply.

A clear distinction can be made between the **content** of an email (text and attachments, Art. 4 (3) (b) ePR) and **metadata** processed for the purposes of transmitting the content (IP address, device ID, email address, user's system, time, date and location of the connection, Art. 4 (3) (c) ePR).

#### 2.4.2.2.1 Content

Art. 6 (1) ePR allows the processing of content by a **service providers** 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".*

There can be no doubt that processing the content of an email is necessary for its transmission. Therefore, the transmission of a mail meets the requirements of Art. 6 (1) (a) ePR. However, filtering mails in order to detect spam mails and malware is clearly not necessary for the transmission so that spam filters do not fall under the permission of Art. 6 (1) (a) ePR.

Spam filters are a means of making mail communication secure and a means of detecting faults and errors. Therefore, Art. 6 (1) (b) ePR applies, and the use of **spam filters** by Gmail is covered by the permission of **Art. 6 (1) (b) ePR**.

There is, however, **also Art. 6 (3) ePR** that allows providers to 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."*

According to Art. 6 (3) (a), the scanning of content by Gmail must be necessary to fulfil the service and, in addition, the end-user has to give his or her consent. If one of these two requirements is not met, processing content is prohibited.

The requirement of the necessity "to fulfil the service" is more or less identical with the requirement in **Art. 6 (1) (a) ePR**. Therefore, for the **consent** requirement to be meaningful, it must be understood to be an **additional requirement** when content is processed by a service provider.

**Art. 6 (3) (b) ePR** appears to refer to the processing of content when such processing is not necessary for the provision of the communications service but serves **other purposes**. In such a case, Art. 6 (3) (b) ePR allows processing under three conditions:

- Making information **anonymous** must be impossible or impracticable.
- There needs to be **consent** by all end-users concerned.
- The **DPA** needs to be consulted before the content is processed, and it is upto the DPA to decide if processing is permitted (Art. 36 (2) and (3) GDPR).

**Spam filters** are not necessary for the transmission of mails. Therefore, it is **Art. 6 (3) (b)** and not Art. 6 (3) (a) ePR that applies to the Gmail spam filters. For the filters to be legal, the "consent by all end-users concerned" is necessary. This raises the **awkward question** if the spammer is one of the "end-users concerned" and if his or her **consent** is necessary[24].

[24] See German Bar Association, Position Paper on the ePR draft, p. 21/22, https://anwaltverein.de/de/newsroom/sn-29-17-stellungnahme-zur-eprivacy-vo.

In Art. 2 (14) EECC (see Art. 4 (1) (b) ePR), the "end-user" is defined as

> "*a user not providing public communications networks or publicly available electronic communications services*".

The "user" is defined in Art. 2 (3) EECC 2016/0288 (COD) ePR as

> "*a legal entity or natural person using or requesting a publicly available electronic communications service*".

The definitions of **"end-user"** and "user" in the EECC do not distinguish between the **sender** and **recipient** of a message. Therefore, Art. 6 (3) (b) ePR would mean that **both** the recipient and the sender of a mail need to give **consent** if spam or malware filters are used. Gmail would be required to ask the spammer for consent.

The requirement to ask the spammer for consent before filtering his or messages for spam mails is not the only inconsistency of Art. 6 (3) (b) ePR[25]:

- **Anonymization** is a requirement that is known from data protection. When there is information or data relating to a person (be it a natural or legal person), anonymization is a means of **protecting privacy**. However, the ePR does not distinguish between personal and non-personal data and protects the confidentiality of data irrespective of its content. **Non-personal information** can, by definition, not be made anonymous so that the anonymization requirement is **inconsistent** with the aims of the ePR[26].
- **Art. 36 (1) GDPR** obliges controllers to consult the DPA prior to processing when a **data protection impact assessment** under Art. 35 GDPR indicates that the processing would result in high risks. There is no obligation of prior consultation without a data protection impact assessment, and there is **not a single scenario** that the GDPR defines for a **prior consultation** to be always necessary. Even when health data or other very sensitive data are processed, a data protection impact assessment may come to the result that there is no high risk (due to protective measures taken by the controller) so that there is no necessity of consulting the DPA. Why such a consultation should always be necessary in the cases of Art. 6 (3) (b) ePR, is entirely unclear.

Until recently, Google automatically scanned emails for the purpose of targeted advertising. This kind of **targeted advertising** was controversial[27], and it is likely to be the intention of Art. 6 (3) (b) ePR to make scanning mails for targeted advertising as difficult as possible. However,

---

[25] See German Bar Association, Position Paper on the ePR draft, p. 20, https://anwaltverein.de/de/newsroom/sn-29-17-stellungnahme-zur-eprivacy-vo.

[26] See German Bar Association, Position Paper on the ePR draft, p. 20, https://anwaltverein.de/de/newsroom/sn-29-17-stellungnahme-zur-eprivacy-vo.

[27] See Google Will No Longer Scan Gmail for Ad Targeting, New York Times of June 23rd, 2017, https://www.nytimes.com/2017/06/23/technology/gmail-ads.html

even for targeted advertising, Art. 6 (3) (b) ePR clearly goes too far. There is no reason why the **automated scanning** (as opposed to reading) of messages should be regarded as **more intrusive than profiling** that is covered by **Art. 22 GDPR**. According to Art. 22 (3)/9 (2) (a) GDPR, even profiling of health and other sensitive data is lawful if the data subject has given explicit consent.[28] Why **Art. 6 (3) (b) ePR** demands **more than consent for data that may not even be personal** is not at all clear.

#### 2.4.2.2.2 Metadata

Article 6 (2) (b) ePR allows service providers to process electronic communications metadata if:

> *"it is necessary for billing, calculating interconnection payments, **detecting or stopping fraudulent, or abusive use of**, or subscription to, **electronic communications services**".*

The filters Gmail uses serve to detect spam and malware to enable an efficient use of the webmail service. Without filtering the metadata of messages, such as the IP and email addresses of senders, an efficient use of Gmail would be severely impaired due to the high amount of spam messages and the danger of malware. The use of filter techniques and the related processing of metadata are necessary for **detecting or stopping the abusive use of webmail services**.

Therefore, the scanning and processing of metadata by Gmail or any other mail provider is lawful without the end-users' consent pursuant to Art. 6 (2) (b) ePR.

### 2.4.2.3 Storage and erasure (Art. 7 ePR)

One of the **main services** Gmail and other email providers offer is the (often unlimited) storage of emails. Moreover, it is typically the **user** who wants (and expects) **control over the erasure of mails**. The user expects to decide himself or herself if and which mails are deleted. The service provider's duty to erase mails is, therefore, incompatible with the reasonable expectations of the users of email services.

Emails often contain personal data. **Art. 17 GDPR** contains extensive provisions on the **erasure** of such data. As far as personal data contained in mails are concerned, there is no reason why specific email provisions should be necessary to supplement the provisions of Art. 17 GDPR. Moreover, there is the right to data **portability (Art. 20 GDPR)**. There is no doubt that Art. 20

[28] See *Buchner* in Kühling/Buchner (ed.), GDPR, 1. Edt. 2017, Art. 22 p. 472.

GDPR applies to email services.[29] When a user wants to change **email providers**, he will not normally want his stored mails erased (Art. 7 ePR) but will have an interest to use his right to data portability pursuant to Art. 20 GDPR.

When emails do not contain personal data but **business information**, the GDPR does not apply. At the same time, it is even more evident that it will normally not be in the **interest of the user** to have his mails deleted. On the contrary, the user will normally expect his **mails to be stored** until he himself decides to delete them.

#### 2.4.2.4 Results

The results of the analysis are as follows:

- **Art. 5 ePR** is **imbalanced** as it regards spam and malware filters as a risk to communication although it is spam and malware that pose risks and not the filters that protect the free flow of communication.
- As far as the **content** of mails is concerned, both Art. 6 (1) (b) and Art. 6 (3) (b) ePR apply. Art. 6 (3) (b) ePR is clearly excessive as it demands the **spammer's consent** for the use of a spam filter. Moreover, for every spam filter, prior consultation of the DPA is obligatory, which is not in line with the provisions of the GDPR. Last but not least, Art. 6 (3) (b) ePR requires the **anonymization of content** even though content may not contain any personal information, which is also incoherent.
- As far is **metadata** are concerned, Art. 6 (2) (b) ePR allows scanning mails for metadata in order to identify malware and spam mails. While this appears to be satisfactory, it is still unclear why IP addresses and other **"online identifiers"** clearly **covered by the GDPR** need to be regulated in the ePR as well.
- **Art. 7 ePR** emphasizes the provider's duty to erase mails although is will typically be the **user's expectation that mails are not erased but stored**. Art. 7 ePR is not in line with Art. 17 and 20 GDPR and with the user's reasonable expectation to be in **control** of the storage or deletion of mails.

- Under the **GDPR**, spam filters may be used when the provision of such filters is part of the provider's contractual duties (Art. 6 (1) (b) GDPR).

[29] See *Herbst* in Kühling/Buchner (ed.), GDPR, 1. Edt. 2017, Art. 20 p. 446.

### 2.4.3 Internet Access: “Wi-Fi Hotspots”

Wi-Fi hotspots are Wi-Fi access points which are available in public facilities, such as airports, railway stations, public institutions, universities, libraries, hotels and shopping centres. These public hotspots are also referred to as **"Open Wi-Fi".** Providers sometimes charge a fee for the use of public hotspots or limit the usage. Therefore hotspot routers have a timer to bill or record the time of the usage. Most hotspots are **unencrypted**, which means that the hotspot provider is (at least, theoretically) able to surveil communication. Some providers encrypt their hotspots with a **password** which appears to be safe[30].

Using the example of an **airport hotspot**, the following analysis shows the effects of the ePR on hotspot providers. To connect to an airport hotspot the user has to select the Airport Wi-Fi network in his device settings and then open a browser. The user then has to register. After registering the user received an email with a link to enter to set up a permanent hotspot account. Alternatively, the hotspot can be used without registration by selecting the "Airport" Wi-Fi network in the WI-FI settings of the device.

Art. 2 (4) EECC (Art. 4 (1) (b) ePR) defines an “electronic communications service” as

> “*[…] 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.*”

Art. 2 (2) Regulation (EU) 2015/2120 defines an “internet access service” as a

> “***publicly available electronic communications service that provides access to the internet****, and thereby connectivity to virtually all end points of the internet, irrespective of the network technology and terminal equipment used*”.

Providers of airport hotspots are providers of access to the internet. Thus, they are provides of an “electronic communications service” within the meaning Art. 4 (1) (b).

[30] An Overview of How WiFi Hotspots Work, updated July 9th, 2014, http://internet-access-guide.com/an-overview-of-how-wifi-hotspots-work/.

#### 2.4.3.1 Confidentiality (Art. 5 ePR)

When a user connects his or her device to the airport hotspot, the hotspot provider uses a network protocol to process **device and connection information** as well as communications **content** in the form of data packages.

Device and connection information contains data such as the device ID, operating system, browser, URLs of visited websites, date, time and duration. Such data will be processed in an electronic communications network for the purposes of transmitting, distributing or exchanging electronic communications content. Thus, the processing of data falls under the definition of "electronic communications **metadata**" (Art. 4 (3) (c) ePR).

If the user uses messenger apps, webmail or VoIP services, communications content will be transmitted via the airport hotspot. The transmitted content can contain data such as text, voice, videos, images, and sound. Such data falls under the definition of "electronic communications **content**" (Art. 4 (3) 3 (b) ePR).

The airport hotspot is a public Wi-Fi access point which processes communications content (e.g. text, voice, videos, images, and sound) and metadata. To provide the service, the hotspot provider has to process such these data. According to **Art. 5 ePR**, such processing is prohibited, except when the end-user has given his consent or it when processing is permitted by the ePR.

The **prohibition** is at odds with the **expectations of the hotspot users**. The purpose of using a hotspot is the transmission of data, be it content or metadata. It is the transmission of data that the user pays for if the hotspot service is not free of charge.

There can be no doubt that there are **risks of interception** when the hotspot service is insecure. Users expect hotspots to be safe from interception so that it is reasonable and adequate that Art. 5 ePR declares both interception and surveillance to be illegal. At the same time, it may be worth noting that there are **no provisions on data security**. The security of networks and services is an issue that is not addressed by the ePR.

Data security was amongst the key issues of the ePD. **Art. 4 (1) ePD** put a general duty on the provider of a publicly available electronic communications service to

> *"take appropriate technical and organisational measures to safeguard security of its services, if necessary in conjunction with the provider of the public communications network with respect to network security. Having regard to the state of the art and the cost of their implementation, these measures shall ensure a level of security appropriate to the risk presented."*

While Art. 4 (1) ePD surely met the reasonable (security) expectations of a hotspot user, the same is not true for the prohibition of processing content and metadata that can be found in Art. 5 (1) ePR.

#### 2.4.3.2 Consent Requirements (Art. 6 ePR)

##### 2.4.3.2.1 Content

Art. 6 (1) and (3) ePR apply to the processing of content. As far as **content** is transmitted when a public hotspot is used, such processing is necessary to achieve the transmission of the communication. Therefore, such **processing** meets the is covered by **Art. 6 (1) (a) ePR**. However, as shown above, it does not suffice to meet the requirements of Art. 6 (1) ePR. In addition, Art. 6 (3) ePR applies to content.

According to **Art. 6 (3) ePR**, hotspot providers 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*".

As shown above, exception (a) applies if processing is necessary for the communications service whereas exception (b) applies to the processing for other purposes than the delivery of the service.

As far as content is concerned that is transmitted by the hotspot provider, such a **transmission** is **necessary** for the service. If a user needs the hotspot to send messages or other content, the transmission of such content is necessary in order to make use of the internet access that the hotspot establishes.

Therefore, **exception (a) applies**, and it is necessary that "the end-user or end-users concerned have given their consent". While it is clear that the hotspot user, as an "end-user" will always agree to the transmission of content, it is unclear if the **recipient** of a message sent via a hotspot connection also qualifies as an **"end-user concerned"**. This would, however, be highly impractical because there is no feasible way how a hotspot provider could identify possible recipients of messages sent via the hotspot and how the provider could seek consent from such recipients.

Exception (a) is not only **unclear** as far as the end-users are concerned whose consent is necessary and **impractical** if it is interpreted as requiring the consent of recipients of messages. Art. 6 (3) (a) is **not consistent with Art. 6 (1) (b) GDPR**.

Art. 6 (1) (b) GDPR permits the processing of personal data, without the data subject's consent, if such

> *"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".*

The strict and clear rule of the **GDPR** is an either/or:[31]

- **Either processing of data is necessary** to perform a contract. Then, consent is not necessary.
- **Or processing of data is not necessary** to perform a contract. Then, consent may be an alternative for the lawfulness of processing but will, in many cases, be regarded as excessive so that **consent** is **invalid** (Art. 7 (4) and Recital 43 GDPR).[32]

Art. 6 (3) **ePR** enacts principles that are entirely different:

- Even when the processing of data is necessary to perform a contract, **consent** is - **always** and without exception – **required** (exception (a)).
- When the processing of data is not necessary to perform a contract, exception (b) applies, and consent is also required without the restrictions on consent that can be found in Art. 7 (4) and Recital 43 GDPR.

The principles of the GDPR clearly appear to be more reasonable as far as the **expectations of the hotspot user** are concerned. It is the purpose of using a hotspot to be able to go online and send messages via the internet. This exactly meets the requirements of Art. 6 (1) (b) GDPR, and there is no reason why the hotspot provider and the user should be burdened with **additional consent procedures**. At the same time, it appears reasonable to be rather restrictive when it comes to the transmission of content that is not necessary for the use of the hotspot and for the transmission of messages. There is no reason why, in such cases, the restrictions on consent that can be found in Art. 7 (4) and recital 43 GDPR should not apply.

[31] See *Buchner/Petri* in Kühling/Buchner (ed.), GDPR, 1. Edt. 2017, Art. 6 p. 221; *Frenzel* in Paal/Pauly (ed.), GDPR, 1. Edt. 2017, Art. 6 p. 90; *Heberlein* in Ehmann/Selmayr (ed.), GDPR, 1. Edt. 2017, Art. 6 p. 280.
[32] See *Buchner/Kühling* in Kühling/Buchner (ed.), GDPR, 1. Edt. 2017, Art. 7 p. 273.

It is not just the consent requirements of the Art. 6 ePR that deviate severely from the GDPR. Also the requirement of **periodic reminders** on the right to withdraw consent in **Art. 9 (3) ePR** deviates from the **GDPR**:

> *"End-users who have consented to the processing of electronic communications data as set out in point (c) of Article 6 (2) and points (a) and (b) of Article 6 (3) shall be given the possibility to withdraw their consent at any time as set forth under Article 7 (3) of Regulation (EU) 2016/679 and be reminded of this possibility at periodic intervals of 6 months, as long as the processing continues."*

No such reminders are required by the GDPR.

#### 2.4.3.2.2 Metadata

In order to operate an airport hotspot and to connect a device to the internet, it is necessary to process IP addresses and other metadata. Such processing of metadata is covered by Art. 6 (1) ePR.

However, there are additional requirements for the processing of metadata in Art. 6 (2) ePR. Art. 6 (2) permits the provider to process communications metadata if processing is necessary for the quality of service (a), for billing (b), or when there is consent (c).

**Art. 6 (2) (a) ePR** allows service providers to process electronic communications metadata if

> "*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*".

Quality of service is dealt with in **Art. 97 EECC and Art. 4 of the Regulation (EU) 2015/2120**. These provisions do, however, not impose quality standards on providers but oblige providers to inform users of quality standards. Which **standards** are actually meant to be "mandatory quality of service requirements" is **unclear**.

**Art. 6 (2) (b) ePR** allows service providers to process electronic communications metadata if

> "*it is necessary for billing, calculating interconnection payments, detecting or stopping fraudulent, or abusive use of, or subscription to, electronic communications services*".

Art. 6 (2) (b) ePR will allow the processing of metadata on the duration of use when this is required for **billing**. Art. 6 (2) (b) ePR will also allow the processing of metadata in order to identify the user (e.g. user names, device IDs) when the use of the hotspot requires a **subscription**. For the safe usage of a hotspot it might also be necessary to process some metadata to detect or stop **fraudulent or abusive use**. The **extensive processing of metadata**, in articular of the IP addresses of websites visited, which is necessary for the operation of a hotspot is, however,

**not covered** by Art. 6 (2) (b) ePR so that the operation of an airport hotspot cannot be based on Art. 6 (2) (b) ePR as far as metadata are concerned.

**Art. 6 (2) (c) ePR** permits the processing of communications metadata if

> "*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**.*".

Different from Art. 6 (3) (a) and (b) ePR, Art. 6 (2) (c) ePR does not distinguish between the processing of metadata that is necessary to provide the service ("specific services") and the processing of metadata that is necessary for other purposes ("specified purposes").

Art. 6 (2) (c) ePR allows processing under two conditions:

- Making information anonymous must be impossible or impraticable.
- There needs to be consent by "the end-user" concerned.

For an airport hotspot this means that the hotspot provider needs the user's consent for processing metadata. Consent will, however, only be valid if it is impossible to anonymize metadata.

The **consent requirement** is not in line with **Art. 6 (1) (b) GDPR**. It is the purpose of using a hotspot to be able to go online, and going online requires, by technical necessity, the processing of metadata. This meets the requirements of Art. 6 (1) (b) GDPR, and there is no reason why the hotspot provider and the user should be required to go through additional consent procedures.

As far as **anonymization** is concerned, the obligation of "processing information that is made anonymous" is as inconsistent with the aims of the ePR as the anonymization requirement for content in Art. 6 (3) (b) ePR. When there is information or data relating to a person, anonymization is a means of protecting privacy. However, the ePR does not distinguish between personal and non-personal data and protects the confidentiality of data irrespective of its content. **Non-personal information** can, by definition, not be made anonymous so that the anonymization requirement is inconsistent with the aims of the ePR.

#### 2.4.3.3 Storage and erasure (Art. 7 ePR)

A hotspot provider will not store content and will store metadata only when such metadata are necessary for billing or for recognizing a registered user.

As for the erasure of metadata, Art. 7 (2) and (3) ePR applies:

> *"(2)* ***Without prejudice to point (b) of Article 6 (1) and points (a) and (c) of Article 6 (2)****, the provider of the electronic communications service shall* ***erase*** *electronic communications* ***metadata or make that data anonymous*** *when it is no longer needed for the purpose of the transmission of a communication.*
>
> *(3) Where the processing of electronic communications metadata takes place for the purpose of* ***billing*** *in accordance with point (b) of Article 6(2), the relevant metadata may be kept until the end of the period during which a bill may lawfully be challenged or a payment may be pursued in accordance with national law."*

Thus, metadata must be **erased** after the use of a hotspot **unless**

- the data are necessary for **security** reasons (Art. 6 (1) (b) ePR), or
- the data are necessary for meeting mandatory **quality of service requirements** (Art. 6 (2) (a) ePR), or
- the data are necessary for **billing** (Art. 6 (2) (b) ePR), or
- the end-user has given his or her **consent** and **anonymization** is **impossibl**e or impractible (Art. 6 (2) (c) ePR).

For the hotspot provider, this means that he may store metadata he needs for billing purposes without the end-user's consent (Art. 7 (3) ePR). For metadata stored in order to recognize a registered user, the provider needs the end-user's consent, such consent only being valid when anonymization is impossible or impracticable (Art. 6 (2) ePR).

The **consent requirement** is **inconsistent with Art. 6 (1) (b) GDPR** and with the user's expectations. When a user registers at an airport hotspot, he will expect easy access to the network the next time he comes to the airport. As far as the storage of metadata is concerned necessary for recognizing the user, consent is a burdensome formality that is unnecessary. As far as anonymization is concerned, the duty to anonymize is, again, not in line with the aims of the ePR.

#### 2.4.3.4 Results

The results of the analysis are as follows:

- Although data security is a major issue for hotspot users, the **ePR does not contain provisions on security** (no provisions similar to Art. 4 (1) ePD).
- Instead, Art. 5 ePR prohibits the processing of data by a hotspot provider even though data processing is necessary to enable the user to go online via the hotspot. **Art. 5 ePR** is **not in line with the expectations of a reasonable hotspot user**.
- As far as the **processing of content** is concerned, Art. 6 (3) (a) ePR applies and obliges the provider to seek consent of "end-users concerned". It is **open to interpretation** if "end-

users concerned" include **third parties** who receive messages sent via the internet access provided by the hotspot. There is no realistic way to obtain consent from such third parties.

- As far as **metadata**, in particular IP addresses, are concerned, processing such metadata requires consent according to Art. 6 (2) (c) ePR. Moreover, Art. 6 (2) (c) ePR requires the anonymization of metadata even though metadata may not contain any personal information, which is also incoherent.
- The **consent requirements contradict Art. 6 (1) (b) GDPR**. The hotspot provider needs to process content as well as metadata for the performance of the contracts with registered users so that consent is not required by the GDPR.
- **Art. 7 (3) ePR also contradicts Art. 6 (1) (b) GDPR**. As far as registered users are concerned, the storage of metadata necessary to recognize such users is covered by Art. 6 (1) (b) GDPR. The user's consent is not required whereas such consent is one of the requirements of Art. 7 (3) ePR.

| |
|---|
| Under the **GDPR**, hotspot providers can rely on Art. 6 (1) (b) GDPR) when there is a contract between the provider and the user. Without such a contract, the processing of data will normally be covered nby "legitimate interests pursuant to Art. 6 (1) (f) GDPR. |

### 2.4.4 Mobile Apps: "OpenTable"

OpenTable is a mobile app which provides a **real-time reservation services for restaurants**[33]. The app contains restaurant descriptions, contact details and opening hours, images, information on price levels, customer reviews and maps. The user can search for restaurants by locationor  by name or type of cuisine and check the availability for the desired time. The user can send a reservation. The reservation will be confirmed by the restaurant by email.

**Art. 2 (5) EECC** defines an "interpersonal communications service" as

> "*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*".

The user sends his reservation to the restaurant which confirms the reservation immediately by email including a reservation code. Thus, OpenTable is a service which enables direct **in-**

[33] See the website: www.opentable.com.

**terpersonal and interactive exchange** of information via an electronic communications networks between the user and the restaurant, whereby the user determines the chosen restaurants as recipients. Thus, OpenTable is an **"electronic communications service"** within the meaning of Article 4 para. 1 (b) ePR/Art. 2 (4) EECC.

When the user sends his or her reservation to the restaurant, content data (restaurant XY, time, number of persons) as well as metadata (IP address, device information, GPS data, date and time of communication) will be transmitted.

#### 2.4.4.1 Confidentiality (Art. 5 ePR)

Art. 5 ePR prohibits the interception and surveillance of data transmitted via the OpenTable app as well as the mere processing of such data. Again, this is **not in line with the users' expectations**. The user will expect the reservations to be secure from interception and surveillance. At the same time, the user will expect the provider to transmit the reservation to the restaurant, which, by necessity means that the user expects data processing. If the processing of data is what the user expects the app provider to do, this expectation contradicts the prohibition imposed on data processing by Art. 5 ePR.

#### 2.4.4.2 Consent Requirements (Art. 6 ePR)

##### 2.4.4.2.1 Content

**Art. 6 (1) ePR** allows the processing of content to the extent such processing is necessary for the transmission of the communication. The transmission of the reservation details to the restaurant owner is, therefore, covered by Art. 6 (1) ePR.

In addition, Art. 6 (3) (a) ePR requires the **consent of the "end-users concerned"**. This may be interpreted to mean that consent is necessary both of the customer (app user) and of the restaurant that receives the reservation.

The strict consent requirement in Art. 6 (3) (a) ePR **contradicts Art. 6 (1) (b) GDPR**. The app provider cannot fulfil his or her contractual duties without transmitting the reservation to the restaurant. Therefore, such transmission is covered by Art. 6 (1) (b) GDPR without the consent of either side (app user/restaurant) being required.

##### 2.4.4.2.2 Metadata

**Art. 6 (1) ePR** allows the processing of metadata when such processing is necessary for the transmission of the communication. To the extent processing of metadata (IP address, device information, GPS data, date and time of communication) is necessary for the processing of OpenTable reservations, such processing is covered by Art. 6 (1) ePR.

In addition, **Art. 6 (2) (c) ePR** requires the consent of the app user, which **contradicts Art. 6 (1) (b) GDPR** to the extent the processing of metadata is necessary for the app provider to fulfil his or her contractual duties.

#### 2.4.4.3 Storage and erasure (Art. 7 ePR)

**Information on previous reservations** is stored by the OpenTable provider in order to enable the user to look up to which restaurants he or she has been. Storage of such information is **part of the servic**e that the app offers and, therefore, covered by **Art. 6 (1) (b) GDPR**. According to the GDPR, the user's consent is not necessary.

**Art. 7 (1) ePR** obliges the OpenTable provider to erase information on previous reservations or make such information anonymous as soon as the restaurant owner has received the reservation. It is worth noting that **anonymization** appears to be an **absurd option** as the information on previous visits to restaurants is of little (if any) use to the app user if the names of the restaurants are made anonymous.

According to Art. 7 (1) and Art. 6 (3) (a) and (b) ePR, storage requires the app user's **consent**. This clearly **contradicts Art. 6 (1) (b) GDPR**.

#### 2.4.4.4 Results

The results of the analysis are as follows:

- The provider of the OpenTable app processes communications data (both content and metadata). Although such processing is exactly what the app user expects, **processing** is, on principle, **prohibited according to Art. 5 ePR**.
- **Art. 6 (2) (c) and Art. 6 (3) (a) ePR** apply and oblige the provider of the OpenTable app to seek the app users' consent to the processing of reservation data and metadata. This is **not in line with Art. 6 (1) (b) GDPR** as Art. 6 (1) (b) GPDR permits processing without consent.
- The **storage of information** on previous restaurant visits is covered by Art. 6 (1) (b) GDPR and does not require consent according to the GDPR whereas, for the same information/content, there is a **consent requirement in Art. 7 (1)/Art. 6 (3) ePR**.

| |
|---|
| Under the **GDPR**, the provider of the OpenTable app will be able to rely on Art. 6 (1) (b) GDPR. |

# 3 Protection of information stored in terminal equipment ("cookie regulation")

## 3.1 Cookie and offline tracking provisions

### 3.1.1 Art. 8 ePR

#### 3.1.1.1 Provisions on cookies

Art. 8 (1) ePR prohibits, as a rule,

> *"the use of processing and storage capabilities of terminal equipment and the collection of information from end-users' terminal equipment, including about its software and hardware".*

According to Art. 2 (14) EECC of the draft Directive establishing the European Electronic Communications Code (EECC[34], Art. 4 (1) (b) ePR) an "end-user" is

> "*a user not providing public communications networks or publicly available electronic communications services*".

"User" is defined in Art. 2 (13) EECC as:

> "*a legal entity or natural person using or requesting a publicly available electronic communications service*".

Based on these definitions, an "end-user" can be a **legal entity** or a **natural person**.

For the definition of "**terminal equipment**", Art. 4 (1) (c) ePR refers to Art. 1 (1) of the Commission Directive 2008/63/EC:

> "*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*".

Thus, the definition of "terminal equipment" encompasses devices such as telephones, smartphones, routers and other internet connected devices such as PCs, laptops, tablets, game consoles, wearables and "IoT" devices.

There are some **exceptions from the "cookie prohibition"** in Art. 8 (1) ePR. According to Art. 8 (1) ePR, the use of cookies and the collection of information from end-users' devices is permitted if

[34] Proposal for a Directive of the European Parliament and of the Council establishing the European Electronic Communications Code (Recast), COM/2016/0590 final - 2016/0288 (COD), http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=comnat:COM_2016_0590_FIN.

*"(a) it is necessary for the sole purpose of carrying out the transmission of an electronic communication over an electronic communications network; or*

*(b) the end-user has given his or her consent; or*

*(c) it is necessary for providing an information society service requested by the end-user; or*

*(d) if it is necessary for web audience measuring, provided that such measurement is carried out by the provider of the information society service requested by the end-user."*

#### 3.1.1.2 Provisions on offline tracking

While the ePD did not contain any provisions on offline tracking, i.e. on **tracking devices** by means of receiving WI-FI, Bluetooth or other signals emitted by such devices, Art. 8 (2) ePR introduces a prohibition of offline tracking.

According to Recital 25 ePR, offline tracking is regarded as **potentially intrusive**, especially when offline tracking is used for **targeted advertising**:

*"Accessing electronic communications networks requires the regular emission of certain data packets in order to discover or maintain a connection with the network or other devices on the network. Furthermore, devices must have a unique address assigned in order to be identifiable on that network. Wireless and cellular telephone standards similarly involve the emission of active signals containing unique identifiers such as a MAC address, the IMEI (International Mobile Station Equipment Identity), the IMSI etc. A single wireless base station (i.e. a transmitter and receiver), such as a wireless access point, has a specific range within which such information may be captured. Service providers have emerged who offer tracking services based on the scanning of equipment related information with diverse functionalities, including people counting, providing data on the number of people waiting in line, ascertaining the number of people in a specific area, etc. This information may be used for* ***more intrusive purposes, such as to send commercial messages to end-users****, for example when they enter stores, with personalized offers. While some of these functionalities do not entail high privacy risks, others do, for example, those involving the tracking of individuals over time, including repeated visits to specified locations. Providers engaged in such practices should display prominent notices located on the edge of the area of coverage informing end-users prior to entering the defined area that the technology is in operation within a given perimeter, the purpose of the tracking, the person responsible for it and the existence of any measure the end-user of the terminal equipment can take to minimize or stop the collection. Additional information should be provided*

*where personal data are collected pursuant to Article 13 of Regulation (EU) 2016/679."*

It is worth noting that intrusions on privacy resulting from the "sending of commercial messages to end-users" are covered by **Art. 16 ePR** ("Unsolicited communications", also Art. 13 ePD). It is unclear why opt-in rules provisions of Art. 16 ePR should not be sufficient for the protection of privacy against offline tracking.

There are only **two exceptions** from the prohibition of offline tracking. Pursuant to Art. 8 (2) ePR, the collection of information emitted by terminal equipment to enable it to connect to another device and/or to network equipment is only permitted if

*"(a) it is done exclusively in order to, for the time necessary for, and for the purpose of establishing a connection; or*

*(b) a clear and prominent notice is displayed informing of, at least, the modalities of the collection, its purpose, the person responsible for it and the other information required under Article 13 of Regulation (EU) 2016/679 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.*

*The collection of such information shall be conditional on the application of appropriate technical and organisational measures to ensure a level of security appropriate to the risks, as set out in Article 32 of Regulation (EU) 2016/679, have been applied."*

### 3.1.2 GDPR

Cookies are also covered by the GDPR.

Recital 30 GDPR explicitly mentions cookies as an example of "**online identifiers**"[35]:

*"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."*

According to Art. 4 (1) GDPR, such "identifiers" are regarded as personal data:

*"'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,*

[35] See also *Klar/Kühling* in Kühling/Buchner (ed.), GDPR, 1. Edt. 2017, Art. 4 (1) p. 132.

*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".*

When cookies qualify as personal data, the processing of such cookies is prohibited unless one of the six exceptions of **Art. 6 GDPR** applies:[36]

*"(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."*

It is worth noting that

- Art. 6 GDPR only applies to cookies that may identify a **natural person** whereas Art. 8 ePR applies to all devices irrespective of a connection to a natural person;
- According to Art. 6 (1) (b) and (f) GDPR both the **performance of a contract** and **legitimate interests** pursued by the controller or by a third party may be reasons for the lawful processing of cookies whereas there are no such exceptions in the ePR.[37]

The fact that the use of cookies does not necessarily require consent under the GDPR[38] whereas consent is the rule under the ePR does not take into account that the GDPR only protects natural persons whose privacy is protected by Art. 7 and 8 of the EU Charter of Funda-

[36] See *Ernst* in Paal/Pauly (ed.), GDPR, 1. Edt. 2017, Art. 4 (1) p. 33; *Klar/Kühling* in Kühling/Buchner (ed.), GDPR, 1. Edt. 2017, Art. 4 (1) p. 132.
[37] See *Buchner/Petri* in Kühling/Buchner (ed.), GDPR, 1. Edt. 2017, Art. 6 p. 229 and p. 252.
[38] See *Buchner/Petri* in Kühling/Buchner (ed.), GDPR, 1. Edt. 2017, Art. 6 p. 229 and p. 252.

mental Rights (ECFR) whereas the protection that the ePR provides extends to "**legal persons**" who cannot rely on the ECFR. If there is a justification for different standards in the GDPR and the ePR, the standards in the ePR would need to be **lower** than in the GDPR and not vice versa.

### 3.2 Consent requirement

As a rule, the use of cookies requires consent according to Art. 8 ePR.

Pursuant to Recital 20 ePR, cookies are regarded as a **major threat** to the "private sphere of end-users", a threat on the same level as spyware, and should therefore only be allowed with the **end-user's consent**:

> *"Terminal equipment of end-users of electronic communications networks and any information relating to the usage of such terminal equipment, whether in particular is stored in or emitted by such equipment, requested from or processed in order to enable it to connect to another device and or network equipment, are part of the private sphere of the end-users requiring protection under the Charter of Fundamental Rights of the European Union and the European Convention for the Protection of Human Rights and Fundamental Freedoms. Given that such equipment contains or processes information that may reveal details of an individual's emotional, political, social complexities, including the content of communications, pictures, the location of individuals by accessing the device's GPS capabilities, contact lists, and other information already stored in the device, the information related to such equipment requires enhanced privacy protection. Furthermore, the so-called* ***spyware, web bugs, hidden identifiers, tracking cookies and other similar unwanted tracking tools*** *can enter end-user's terminal equipment without their knowledge in order to gain access to information, to store hidden information and to trace the activities. Information related to the end-user's device may also be collected remotely for the purpose of identification and tracking, using techniques such as the so-called 'device fingerprinting', often without the knowledge of the end-user, and may seriously intrude upon the privacy of these end-users. Techniques that surreptitiously monitor the actions of end-users, for example by tracking their activities online or the location of their terminal equipment, or subvert the operation of the end-users' terminal equipment pose a serious threat to the privacy of end-users.* ***Therefore, any such interference with the end-user's terminal equipment should be allowed only with the end-user's consent and for specific and transparent purposes****".*

### 3.2.1 "Legal persons"

If it is the "private sphere" that is to be protected against tracking cookies and if, as a rule, tracking cookies may only be used with the end-user's consent and for specific and transparent purposes, it is unclear what this means when devices are not owned by a natural person but by a company or a government agency ("legal person"):

- When, e.g., cookies are installed on devices that the police use, the "private sphere" of the owner of the device ("legal person", police) cannot be at stake as the "private sphere" can only be affected when there is a **private individual** who is affected by the cookie. Art. 7 and 8 of the ECFR protect the privacy of EU citizens but **not the "private sphere" of "legal persons"**, companies or government officials or agencies. "Legal persons" do not have a "private sphere" that can (or needs to) be protected.
- When a device is owned by a "legal person", consent requirements mean that it is the **legal representatives of the "legal person"** and not the individuals using the devices who need to be asked for **consent**. In a company that owns smartphones used by employees, this would mean that it is the CEO of the company and not the employees whose consent is relevant. Even if it were argued that the "private sphere" of the employees is at stake, the requirement of the **CEO's consent** can hardly be regarded as an adequate means of protecting the employees' privacy.

### 3.2.2 Cookie banners and browser settings

Both the GDPR and the ePR contain provisions on (avoiding) cookie banners and on browser settings for cookies

**Recital 32 GDPR** contains rules that apply to cookies:

> *"Consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement.* ***This could include 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.*** *Silence, pre-ticked boxes or inactivity should not therefore constitute consent. Consent should cover all processing activities carried out for the same purpose or purposes.* ***When the processing has multiple purposes, consent should be given for all of them. If the data subject's consent is to be given following a request by electronic means, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided."***

As far as consent is concerned, this clearly means:

- **Cookie banners** need to be avoided as they are "unnecessarily disruptive to the use" of the website.[39]
- If at all possible, consent should be given through the **browser settings** ("technical settings for information society services").[40]

Similar to Recital 32 GDPR, cookie banners are to be avoided, and consent given via the browser settings is preferred according to **Recital 22 ePR**:

> *"The methods used for providing information and obtaining end-user's consent should be as user-friendly as possible. Given the ubiquitous use of tracking cookies and other tracking techniques, end-users are increasingly requested to provide consent to store such tracking cookies in their terminal equipment. As a result,* ***end-users are over-loaded 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…"*

Also according to recital 22 ePR, the browsers are regarded as "gatekeepers" that should be used to "prevent" the storing of cookies:

> *"More particularly web browsers may be used as* ***gatekeepers****, thus helping end-users to* ***prevent*** *information from their terminal equipment (for example smart phone, tablet or computer) from being accessed or stored."*

This is clearly **contradictory**: Browser setting cannot at the same time be regarded as

- "**user-friendly**", making it easier for the user to give consent to the storage of cookies and as
- "**gatekeepers**", preventing cookies from being stored.

When web browsers are seen as "gatekeepers" and when restrictive browser settings are encouraged, the provider of a service that depends on the use of cookies will have no choice but to use cookie banners to seek consent every time a user wants to use the service even though his or her browser settings do not permit the storage of cookies. Restrictive browser settings

[39] See *Schantz* in Schantz/Wolff (ed.), GDPR, 1. Edt. 2017, p. 161.
[40] See *Schantz* in Schantz/Wolff (ed.), GDPR, 1. Edt. 2017, p. 160; *Buchner/Kühling* in Kühling/Buchner (ed.), GDPR, 1. Edt. 2017, Art. 7 p. 276.

will, therefore, lead to an **excessive use of cookie banners** – an outcome that both the GDPR and the ePR explicitly aim to avoid.

### 3.3 Browser provisions

Art. 10 (1) ePR requires the providers of **web browsers** and other "software placed on the market permitting electronic communications" to

> *"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."*

#### 3.3.1 Consequences for apps

While the main focus of Art. 10 ePR clearly lies on web browsers, there are various other software products and applications that Art. 10 ePR covers. This is mainly true for **apps**. Many apps "permit electronic communication", for example

- **messenger apps**;
- interactive **gaming apps**;
- **e-commerce apps**.

It is the purpose of such apps to **exchange information**, and it is therefore unreasonable to oblige app providers to prevent the storing of such information. There is no reason why the providers of the **Snapchat** app should be obliged to enable their customers to prevent the storing of pictures on their smartphones when Snapchat is installed although the receipt and (temporary) storage of pictures is the main purpose of the app.

#### 3.3.2 "Third parties"

The term "third parties" is misleading as it is unclear whether the duty to prevent the storage of information means

- generally, the storage of **all cookies** by ("third") persons who are neither the user nor the browser provider ("reject all cookies") or
- the storage of "**third person cookies**" ("reject third party cookies") which would mean that only the storage of "first party cookies" does not need to be preventable.

**Recital 23 ePR** stresses the obligation to offer a "reject third party cookies" option:

> *"The principles of data protection by design and by default were codified under Article 25 of Regulation (EU) 2016/679. Currently, the default settings for cookies are set in most current browsers to 'accept all cookies'. Therefore providers of software enabling the retrieval and presentation of information on the internet should have an* ***obligation to configure the software so that it offers the option to prevent third parties from storing information on the terminal equipment; this is often presented as 'reject third party cookies'****. End-users should be offered a set of privacy setting options, ranging from higher (for example, 'never accept cookies') to lower (for example, 'always accept cookies') and intermediate (for example, 'reject third party cookies' or 'only accept first party cookies'). Such privacy settings should be presented in an easily visible and intelligible manner."*

**Recital 24 ePR** also emphasizes the risks of third party cookies and, therefore, indicates that "reject third party cookies" should be the **default option**:

> *"For web browsers to be able to obtain end-users' consent as defined under Regulation (EU) 2016/679, for example, to the storage of third party tracking cookies, they should, among others, require a clear affirmative action from the end-user of terminal equipment to signify his or her freely given, specific informed, and unambiguous agreement to the storage and access of such cookies in and from the terminal equipment. Such action may be considered to be affirmative, for example, if* ***end-users are required to actively select 'accept third party cookies'*** *to confirm their agreement and are given the necessary information to make the choice. To this end, it is necessary to require providers of software enabling access to internet that, at the moment of installation, end-users are informed about the possibility to choose the privacy settings among the various options and ask them to make a choice. Information provided should not dissuade end-users from selecting higher privacy settings and should include relevant information about the risks associated to allowing third party cookies to be stored in the computer, including the compilation of long-term records of individuals' browsing histories and the use of such records to send targeted advertising. Web browsers are encouraged to provide easy ways for end-users to change the privacy settings at any time during use and to allow the user to make exceptions for or to whitelist certain websites or to specify for which websites (third) party cookies are always or never allowed."*

All in all, Recitals 23 and 24 ePR can be understood as prescribing "reject third party cookies" as the standard default option of web browsers. However, the wording of **Art. 10 (1) ePR** is **unclear** and also open to the interpretation that no distinction is made between first and third party cookies so that the standard default option needs to be "reject all cookies".

## 3.4 Case Studies

### 3.4.1 Google Analytics

Google Analytics is an **analytics tool** that tracks and analyses the web traffic. By using Google Analytics, the operator of a website gets information on the number of visitors and on the most popular pages of his or her website. Moreover, Google Analytics analyses visitors' IP adresses in order to find out which countries and regions users come from. Also, the pages that visitors previously used and the landing pages are analysed.

According to a recent study, the web analytics market was estimated at $1.3 billion in 2015 and is expected to reach $4.9 billion by 2022[41].

The core of the Google Analytics functions is a small piece of code. This piece of code is inserted into the HTML code on each page of the website and is always loaded when a user calls the page. Once a cookie is installed on the user's device and the snippet is active, the cookie sends Google information on the use of the website[42].

**Cookies** are small text files which are stored in the user's device when using a website. After the initial storage of the cookie, data may be stored over several sessions within the cookie itself, such as identifiers. The stored data will contain information about the browser type, language settings, visited websites or viewed products.

Google Analytics has an online interface in order to process, analyse and aggregate data. Through several filter options, the data can be analysed and interpreted under different aspects[43].

The Google Analytics tool can be divided into three parts[44]:

- **Collection**: collection of usage data on the website by storing cookies on devices;
- **Processing**: processing of data for storage, analysis and visualization;
- **Configuration**: individual settings for an optimized analysis.

[41] See Web Analytics - Global Market Outlook (2016-2022), https://www.wiseguyreports.com/reports/1184370-web-analytics-global-market-outlook-2016-2022.
[42] https://developers.google.com/analytics/devguides/collection/analyticsjs/cookie-usage.
[43] https://www.google.com/intl/de_ALL/analytics/features/analysis-tools.html.
[44] https://www.google.com/intl/en_uk/analytics/analytics/features/.

#### 3.4.1.1 "Cookie prohibition"

As cookies are stored on the end-users' devices, there can be no doubt that Art. 8 ePR applies to Google Analytics. Therefore, the use of Google Analytics is only lawful if one of the four exceptions provided for in Art. 8 (1) ePR applies.

##### 3.4.1.1.1 Exception for "web audience measuring" (Art. 8 (1) (d) ePR)

In Recital 21 ePR, cookies are recognized as a **"legitimate and useful tool"** for measuring web traffic:

> *„Cookies can also be a legitimate and useful tool, for example, in measuring web traffic to a website."*

According to Art. 8 (1) (d) ePR, the storage of cookies is permitted without the user's consent if:

> *„ it is necessary for **web audience measuring**, provided that such measurement is carried out by the provider of the **information society service** requested by the end-user."*

A definition of "**information society service**" can be found in Art. 1 (1) (b) of the Directive (EU) 2015/1535[45] and can be summarised as a **service provided via the internet.** Therefore, it needs to be the operator of the website as "service provider" who sets the cookies for the exception of Art. 8 (1) (d) ePR to apply.

When the operator of a website uses Google Analytics, it is not the website operator who sets the cookies but Google. Thus, Google Analytics is **not covered** by the exception of Art. 8 (1) (d) ePR.

Art. 8 (1) (d) ePR is **not consistent** with the recognition of web analytics tools as "legitmate and useful" in Recital 21 ePR. The **scope of the exception** is so **narrow** that hardly any analytics tool will be covered by the exception. In theory, a website operator might program and use his or her own analytics tool and then rely on the exception of Art. 8 (1) (d) ePR. In reality, he or she will, however, always use a standard program like Google Analytics provided by a third party so that he or she will not be covered by the "web audience measuring" exception.

It is worth noting that, in the ePD, there was no explicit provision for web analytics. Consequently, no difference was made between analytics tools operated by the website provider (Art. 8 (1) (d) ePR) and analytics tools provided by Google or other third parties.

---

[45] Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services, http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex:32015L1535.

#### 3.4.1.1.2 Consent (Art. 8 (1) (b) ePR)

As the exceptions of Art. 8 (1) (a) and (c) ePR do not apply either, the only way the use of Google Analytics can be lawful is by the **consent of each and every visitor** of the website whose visit is analysed by storing cookies on his or her device.

Like Art. 8 (1) (b) ePR, Art. 5 (3) ePD also required consent for the storage of cookies. Therefore, it has been the opinion of DPAs that the use of Google Analytics under current law also requires the consent of the users affected by analytics cookies. However, DPAs would accept consent through **browser settings** if, at the same time, Google enters into a contract with the operator of the website and agrees to process the analytics data as a mere (order) **processor** following the instructions of the operator as **controller**[46].

Now that a strict consent rule is introduced by the ePR for the use third-party analytics tools and no reference is made to the (order) processing provisions in **Art. 28 and 29 GDPR**, it becomes unclear if the combination of cookie-friendly browser settings and (order) processing will still be a sound basis for the lawful use of Google Analytics and other analytics tools provided by third parties.[47]

#### 3.4.1.2 Consent requirements

As Art. 8 (1) (b) ePR requires the consent to the use of cookies by all users affected, according to Art. 9 (1) ePR, the definition and conditions for the consent of the **GDPR** apply (Art. 4 (11) and Art. 7 GDPR). Thus, it is necessary to seek the "freely given, specific, informed and unambiguous indication of the data subject's wishes". Consent must, moreover, be by a declaration or an "affirmative action" (Art. 4 (11) GDPR). It must not be "unnecessarily disruptive" and can be given by choosing appropriate browser settings (Recital 32 GDPR and Art. 9 (2) ePR).[48]

In **Recital 23 ePR**, **three different standards** are suggested for browser settings:

> *„End-users should be offered a set of privacy setting options, ranging from higher (for example, '**never accept cookies**') to lower (for example, '**always accept cookies**') and intermediate (for example, 'reject third party cookies' or '**only accept first party cookies**').“*

The provider of an analytics tool will not be permitted to track users who choose the higher or the intermediate browser settings as the cookies he will need to use are "**third party cookies**". Therefore, the use of Google Analytics will be limited to users who

- explicitly agreed to "**lower privacy**" **or**

---

[46] See the Guidelines of the Hamburg DPA, Hinweise des HmbBfDI zum Einsatz von Google Analytics, https://www.datenschutz-hamburg.de/uploads/media/GoogleAnalytics_Hinweise_fuer_Webseitenbetreiber_in_Hamburg_2017.pdf

[47] See *Schantz* in Schantz/Wolff (ed.), GDPR, 1. Edt. 2017, p. 160.

[48] See *Schantz* in Schantz/Wolff (ed.), GDPR, 1. Edt. 2017, p. 161.

- explicitly gave **consent** to the use of the tracking tool.

The operator of a website who wants to use Google Analytics comprehensively (i.e. not only for "lower privacy" visitors) will have to use **cookie banners** to seek consent.

#### 3.4.1.3 Results

The results of the analysis are as follows:

- As Google Analytics uses cookies, the prohibition of Art. 8 (1) ePR applies.
- The operator of a website who intends to use Google Analytics cannot rely on the exception of Art. 8 (1) (d) ePR as the exception does not apply to third-party analytics tools like Google Analytics.
- Therefore, the use of Google Analytics requires the **consent** of the visitors of the website pursuant to Art. 8 (1) (b) ePR.
- Consent can be given via the settings of the web browser that the user has installed (Art. 9 (2) ePR). However, Recital 23 ePR recommends standard settings that will only allow third-party cookies if the user explicitly opts for "lower" privacy settings.
- Therefore, the operator of a website will need to ask users individually for their consent if he or she wants their visits to be analysed although their browser settings are not on "lower privacy". This will lead to **recurring cookie banners** and an "**overload of (consent) requests**" although such an "overload" is to be avoided according to Recital 22 ePR.
- There are **inconsistencies between the ePR and the GDPR**. In particular, analytics tools are recognized as "legitimate and useful" tools in Art. 21 ePR. Still, there is no provision that allows the use of cookies because of the website operator's **"legitimate interest**". There is a "legitimate interest" provision in Art. 6 (1) (f) GDPR but no such provision in the ePR. Moreover, it is unclear if and to what extent the provider of the analysis tool (e.g. Google) can be regarded as a mere (order) **processor** having to follow the website operator's instructions pursuant to **Art. 28 and 29 ePR**.

Under the **GDPR**, Google Analytics may be used when the operator of the website can show that he has a "legitimate interest" that outweighs the interest of data subjects (Art. 6 (1) (f) GDPR). This provision allows a flexible approach, taking into account measures that have been taken in order to protect the users' privacy, e g. processor agreements pursuant to Art. 28 GDPR.

### 3.4.2 Browser Fingerprinting

Fingerprinting is a process that recognizes a device after a visit. It is a **non-cookie based tracking method** which uses the unique characteristics of hardware and software features of a computer system. There are two types of fingerprinting: browser fingerprinting and canvas fingerprinting[49].

Information that can be used for **browser fingerprinting** may include the browser version, operating system and version, language and country settings, time zone, installed plug-ins and fonts and the monitor resolution. The log-in status on Facebook or other social platforms may also be used. Even though the attributes by themselves are shared by numerous devices, they can be bundled into a **unique identifier**, an individual "fingerprint" of the user. With this key, a browser can be re-identified[50].

#### 3.4.2.1 "Cookie prohibition"

Browser fingerprinting is a method of collecting information from (browser) software that is stored on the user's device[51]. Such fingerprinting therefore falls in the scope of Art. 8 (1) ePR and is prohibited unless the user has given consent or one of the other exceptions provided for in Art. 8 (1) ePR applies.

Fingerprinting is explicitly mentioned in Recital 21 ePR a serious intrusion on privacy:

> "*Information related to the end-user's device may also be collected remotely for the purpose of identification and tracking, using techniques such as the so-called **'device fingerprinting'**, often without the knowledge of the end-user, and may seriously intrude upon the privacy of these end-users."*

When fingerprinting is used for audience measurement purposes, such a use is not covered by **Art. 8 (1) (d) ePR** as the website operator will not create the "fingerprint" himself but rely on a **service provider** as a **third party** collecting the necessary browser information and producing the "fingerprint".

---

[49] See Federal Association of Digital Business (Bundesverband Digitale Wirtschaft - BVDW), Whitepaper - Browser cookies and alternative tracking technologies: Technical and data protection aspects, September 2015, page 15 http://www.bvdw.org/fileadmin/downloads/cookie-richtlinien/whitepaper_targeting_browsercookies-und-alternative-trackingtechnologien_2015-3.pdf.

[50] Federal Association of Digital Business (Bundesverband Digitale Wirtschaft - BVDW), Whitepaper - Browser cookies and alternative tracking technologies: Technical and data protection aspects, September 2015, page 13 http://www.bvdw.org/fileadmin/downloads/cookie-richtlinien/whitepaper_targeting_browsercookies-und-alternative-trackingtechnologien_2015-3.pdf.

[51] Federal Association of Digital Business (Bundesverband Digitale Wirtschaft - BVDW), Whitepaper - Browser cookies and alternative tracking technologies: Technical and data protection aspects, September 2015, page 13 http://www.bvdw.org/fileadmin/downloads/cookie-richtlinien/whitepaper_targeting_browsercookies-und-alternative-trackingtechnologien_2015-3.pdf.

As the exceptions of Art. 8 (1) (a) (c) ePR do not apply, either, the lawfulness of browser fingerprinting clearly depends on the users' **consent** (Art. 8 (1) b (b) ePR).

#### 3.4.2.2 Consent requirements

For fingerprinting, the same consent requirements apply as for the use of cookies. In particular, **Art. 9 (2) ePR** applies:

> *"Without prejudice to paragraph 1, where technically possible and feasible, for the purposes of point (b) of Article 8(1), consent may be expressed by using the appropriate technical settings of a software application enabling access to the internet."*

Where "possible and feasible", the provider of fingerprinting services needs consent expressed by **browser settings**. However, such consent will only be valid if the user has been **extensively informed** about the technology that is to be used, as provided for in **Recital 24 ePR**:

> *"For web browsers to be able to obtain end-users' consent as defined under Regulation (EU) 2016/679, for example, to the storage of third party tracking cookies, they should, among others, require a clear affirmative action from the end-user of terminal equipment to signify his or her freely given, specific informed, and unambiguous agreement to the storage and access of such cookies in and from the terminal equipment. Such action may be considered to be affirmative, for example, if end-users are required to actively select 'accept third party cookies' to confirm their agreement and are given the necessary information to make the choice. To this end, it is necessary to require providers of software enabling access to internet that, at the moment of installation, end-users are informed about the possibility to choose the privacy settings among the various options and ask them to make a choice.* ***Information provided should not dissuade end-users from selecting higher privacy settings and should include relevant information about the risks associated to allowing third party cookies to be stored in the computer, including the compilation of long-term records of individuals' browsing histories and the use of such records to send targeted advertising.*** *Web browsers are encouraged to provide easy ways for end-users to change the privacy settings at any time during use and to allow the user to make exceptions for or to whitelist certain websites or to specify for which websites (third) party cookies are always or never allowed."*

Thus, in order to obtain consent by browser settings, the user needs to be informed extensively about the way browser fingerprinting works as well as about the risks of fingerprinting. For a number of reasons, this appears **unrealistic**:

- Browser fingerprinting involves **complex technology**, and it will be a challenge to explain how it works in terms an average uses will be able to understand.

- As far as cookies are concerned, Recital 24 ePR contains fairly detailed guidelines how users should be informed about the use of cookies and the risks to privacy resulting from cookie consent. There are **no statutory guidelines** how to inform users as far as other tracking methods are concerned.
- Art. 10 ePR and Art. 9 (2) ePR are worded in a "**technology neutral**" way. The consent mechanism described in Art. 10 ePR and Art. 9 (2) ePR is meant to work not only for cookies but also for fingerprinting and other tracking methods. However, Recital 24 ePR shows how much the wording of Art. 10 ePR and Art. 9 (2) ePR is **focussed on cookies**.
- For many years browsers have been equipped with **cookie settings**, and **standards** have been established for such settings. Recitals 23 and 24 ePR are based on these standards. There are, however, no such standards for other tracking technologies. Providers of such technologies therefore not only lack guidance in the ePR as to how consent can be obtained by browser setting but they also **lack industry standards** and will depend on browser providers to develop such standards.
- Art. 10 and Recitals 23 and 24 ePR impose detailed obligations on browser providers as far as cookie settings are concerned. It remains to be seen if there are **sufficient incentives for browser providers** to create standard settings for fingerprinting and other non-cookie tracking technologies. From the point of view of a browser provider, additional settings and, especially, additional duties to inform users about the exact details and risks of such settings will not enhance the **user-friendliness** of the browser.
- Even if standards for browser fingerprint settings similar to cookie settings will be established one day, this will take time. At least for the time being, the only way the consent to fingerprinting necessary pursuant to Art. 8 (1) (b) ePR can be obtained, will realistically be **individual consent**. This will contribute to an "**overload of requests**" that Recital 22 aims to prevent.
-

#### 3.4.2.3 Results

The results of the analysis are as follows:

- Fingerprinting falls under the "cookie provision" of Art. 8 ePR and requires **consent** pursuant to Art. 8 (1) (b) ePR.
- For the time being, it does not appear to be realistic to expect that there will be **browser settings** on the market soon that meet the requirements of consent for fingerprinting. There are presently **no standards** for such settings, and the standards that can be found in Recitals 23 and 24 ePR focus exclusively on cookies and neglect fingerprinting and other non-cookie tracking technologies.
- At the end of the day, **individual consent** will, for the time being, remain the **only realistic option** for obtaining users' consent to fingerprinting. This will encourage the use of **cookie**

**banners**, although cookie banners are disruptive (Recital 32 GDPR),[52] and an "overload of requests" can be counter-productive when it comes to the protection of privacy (Recital 22 ePR).

Under the **GDPR**, browser fingerprinting may be lawful when the provider can show that he has a "legitimate interest" that outweighs the interest of data subjects (Art. 6 (1) (f) GDPR). This provision allows a flexible approach, and it avoids the use of cookie banners.

### 3.4.3 Wi-Fi and Bluetooth Tracking

Mobile phones can be identified by their **MAC (Media-Access-Control) address**, which is a unique serial number, which comes with every WI-FI chip ex factory and cannot easily be changed. If the Wi-Fi function is activated on a smartphone, tablet or laptop, it automatically searches for networks in the environment and sends out radio signals including the MAC address. The MAC address is automatically transmitted when it searches for WI-FI networks in the environment even when the device is not logged in the network[53].

The radio signals emitted by the device can be intercepted and analyzed. Modern routers often have several antennas and can determine in which direction and at what distance a device can be found. If several **WI-FI routers** are activated, the position of a device can be determined to a few meters.

**Bluetooth** can also be used to locate devices offline via "**beacons**". A beacon transmits a unique identifier (**UID**). Like MAC addresses, UIDs cannot be changed easily.

Bluetooth transmitters send their UID to their immediate surroundings and have a range of approximately 30 meters. When a smartphone receives the signal and a specific (e.g. shop) **app** is installed on the phone, this can trigger any action from **targeted advertising** to the display of a location plan. If the user has not installed the app, nothing happens and the smartphone ignores the signal[54].

Beacons are not only used for advertising but for a whole range of other purposes like, for example, for the **monitoring of traffic**. Small Bluetooth transmitters (sensors) are used to locate car radios, navigation devices and smartphones. The location data are used to analyze the

[52] See *Schantz* in Schantz/Wolff (ed.), GDPR, 1. Edt. 2017, p. 161.
[53] Federal Association of Digital Business (Bundesverband Digitale Wirtschaft - BVDW), Proximity Solutions – Smart Technologies for Digital Touch Points, September 2016, page 21 http://www.bvdw.org/mybvdw/media/download/bvdw-leitfaden-proxisolu-20160909.pdf?file=4041.
[54] See WiFi vs. Beacons — Which Is The Better Option For Location Based Services?, Fossbytes, Aug 17th, 2017, https://fossbytes.com/wifi-beacons-better-location-based-services-lbs/

traffic situation on the basis of the time it takes for a device to travel from one measuring point to the next[55].

#### 3.4.3.1 "Tracking prohibition"

For Wi-FI and Bluetooth tracking, there was no provision in the ePD. Art. 5 (3) ePD only covered

> *"the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user".*

Such "storing of information" and "gaining of access to information" is now covered by Art. 8 (1) ePR whereas **Art. 8 (2) ePR** is entirely **new**:

> "*The collection of information emitted by terminal equipment to enable it to connect to another device and, or to network equipment shall be prohibited, except if:*
>
> *(a) it is done exclusively in order to, for the time necessary for, and for the purpose of establishing a connection; or*
>
> *(b) a clear and prominent notice is displayed informing of, at least, the modalities of the collection, its purpose, the person responsible for it and the other information required under Article 13 of Regulation (EU) 2016/679 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.*
>
> *The collection of such information shall be conditional on the application of appropriate technical and organisational measures to ensure a level of security appropriate to the risks, as set out in Article 32 of Regulation (EU) 2016/679, have been applied*

Wi-FI and Bluetooth tracking tools do neither store information on users' devices nor do they gain access to such information so that Art. 8 (1) ePR does not apply. The tools do, however, collect information emitted by devices (MAC addresses; UIDs) and, therefore, fall under Art. 8 (2) ePR.

#### 3.4.3.2 Absence of consent and device setting provisions

WI-FI and Bluetooth tracking tools collect MAC addresses and UIDs for other purposes than merely for the purpose of establishing a connection. Thus, the exception of Art. 8 (2) (a) ePR does not apply.

---

[55] Federal Association of Digital Business (Bundesverband Digitale Wirtschaft - BVDW), Proximity Solutions – Smart Technologies for Digital Touch Points, September 2016, page 21 http://www.bvdw.org/mybvdw/media/download/bvdw-leitfaden-proxisolu-20160909.pdf?file=4041.

Moreover, it is worth noting that consent will not justify WI-FI or Bluetooth tracking. In contrast to Art. 8 (1) (b) ePD, there is **no consent provision** in Art. 8 (2) ePD. From the perspective of a company that intends to use a WI-FI or Bluetooth tracking tool, this means that obtaining users' consent is not an option. This is **grossly inconsistent** with Art. 8 (1) ePD and contradicts the apparent intention of the ePR to make sure that users are in control of data stored on (or emitted by) their devices.

Moreover, according to **Recital 25 ePR**, offline tracking tools are not regarded as services that will always

> *"entail high privacy risks…".*

This is not in line with the absence of consent as legal ground of processing even though **consent** is supposed to be

> *"**a central lawful ground** of this Regulation"*[56].

As there are no provisions on consent there are **no provisions on device settings**, either. Device settings would be an obvious parallel to the browser settings provided for in Art. 9 (2) ePD. It is **absurd** that there can be browser settings permitting the use of cookies but no device setting allowing the tracking of devices by WI-FI or Bluetooth tracking tools.

#### 3.4.3.3 "Prominent notices"

The only option that a service provider has for lawful WI-FI and Bluetooth tracking is "a clear and prominent notice" that meets the requirements of Article 8 (2) (b) ePR, which is explained in Recital 25 ePR:

> "*Providers engaged in such practices should display prominent notices located **on the edge of the area of coverage** informing end-users prior to entering the defined area that the technology is in operation within a given perimeter, the purpose of the tracking, the person responsible for it and the existence of any measure the end-user of the terminal equipment can take to minimize or stop the collection. Additional information should be provided where personal data are collected pursuant to Article 13 of Regulation (EU) 2016/679*".

"Prominent notices located of the area of coverage" are an option when WI-FI or Bluetooth tracking is limited to a certain building (e.g. shop) or area (e.g. surroundings of a shopping mall). However, tracking is not necessarily limited to such an area. This is especially the case when **traffic** is monitored by Bluetooth tracking. In the city of Aarhus in Denmark, tracking traffic data, based on the movement of Bluetooth devices, has proved to be a successful way

[56] Explanatory Memorandum of the draft ePR, p. 9.

of studying the impact of construction projects, roadworks, traffic accidents and traffic lights[57]. Sensors are embedded in traffic lights and roads and there is no (limited) area, at the edges of which "prominent notices" could be placed.

The same is true for the rapidly developing **Bluetooth tracking networks** like Tile. Tile is a small Bluetooth sensor that is attached to objects that a user does not want to lose (e.g. car keys, wallets, phones or sunglasses). If the user is looking for the object, he or she can activate the Tile network by the Tile app. As soon as another user of the Tile app walks passed the object, the object is located and the owner is informed[58]. Quite evidently, there is not the slightest possibility to define appropriate locations for "prominent notices" when such a (potentially global) tracking network is in place.

#### 3.4.3.4 GDPR

MAC addresses and UIDs are covered by the GDPR as they are "**identification numbers**" especially mentioned in Art. 4 (1) GDPR.[59] Such data may be processed when there is consent or when processing is necessary for fulfilling a contract or for the purpose of legitimate interests pursuant to **Art. 6 (1) GDPR**.[60] These are **comprehensive and much more balanced provisions** for the processing of MAC addresses and UIDs than the provisions in Art. 8 (2) ePR.

#### 3.4.3.5 Results

As for WI-FI and Bluetooth tracking, the results of the analysis are as follows:

- Both WI-FI and Bluetooth tracking fall in the scope of Art. 8 (2) ePR. Tracking is therefore prohibited unless one of the two exceptions applies that Art. 8 (2) ePR provides for.
- "Establishing a connection" is not the purpose of WI-FI and Bluetooth tracking. Therefore, such tracking is not covered by Art. 8 (2) (a) ePR.
- **Consent is not an option** as Art. 8 (2) ePR – unlike Art. 8 (1) ePR - lacks a consent exception. This is not in line with the intention of making consent the "central legal ground" of the ePR.
- As consent is not an option, there is also no option to limit the lawful use to users whose device settings allow the emission of WI-FI and Bluetooth signals. While browser settings

[57] Do new roads boost the economy? The science is still finding its way, The Guardian, August 30th, 2017, https://www.theguardian.com/public-leaders-network/2017/aug/30/new-roads-boost-economy-science.
[58] This startup is cashing in on our forgetfulness, CNN Money of Aug. 8th, 2017, http://money.cnn.com/2017/08/08/technology/tile-sport-style/index.html.
[59] See *Klar/Kühling* in Kühling/Buchner (ed.), GDPR, 1. Edt. 2017, Art. 4 (1) p. 132.
[60] See *Buchner/Petri* in Kühling/Buchner (ed.), GDPR, 1. Edt. 2017, Art. 6 p. 229 and p. 252.

are a central element in the proposed rules on cookies and even though every device has an "on/off" button both for WI-FI and for Bluetooth signals, the **device settings do not play any role** in the proposed offline tracking regulation (Art. 8 (2) ePR).

- The obligation to display "prominent notices" (Art. 8 (1) ePR) limits the lawfulness of WI-FI and Bluetooth tracking to tracking tools that monitor a building or a pre-defined area. Important fields of use of the technology like traffic monitoring and Bluetooth networks do not allow the definition of a geographical area of use and the display of "prominent notices". Art. 8 (2) (b) ePR, therefore, **severely impedes** the **further development of offline tracking tools** although Recital 25 ePR concedes that there are areas of use void of high privacy risks.
- Both WI-FI and Bluetooth tracking are covered by the provisions of the **GDPR**. "Identification numbers" are explicitly mentioned in the list of (possibly) personal data in Art. 4 (1) GDPR. The comprehensive rules on the processing of such data in Art. 6 (1) GDPR are **far more balanced and risk-orientated** than Art. 8 (2) ePR.

Under the **GDPR**, WI-FI and Bluetooth tracking are lawful when such tracking is either covered by a contract (Art. 6 (1) (b) GDPR, or when the service provider can show that he has a "legitimate interest" that outweighs the interest of data subjects (Art. 6 (1) (f) GDPR). This provision allows a more flexible approach, taking into account the exact purpose of tracking and the degree to which there are risks for data subjects (risk-based approach).

# 4 Consequences for connected and autonomous cars

## 4.1 Communications technologies in connected cars

Connected and autonomous cars[61] rely heavily on **communications technology** as three examples show:

- In the US state of **Ohio**, a 35-mile stretch from Columbus west to East Liberty, is designed to be the longest **"autonomous-ready" highway** in the country. When finished, the road is to be equipped to be ready for driverless traffic. Sensors will be installed along the highway next year to make it fully operational. The sensors will be able to communicate with autonomous cars, using the **Wi-Fi connection** to inform the con-

[61] See Resolution on Data Protection in Automated and Connected Vehicles, 39th International Conference of Data Protection and Privacy Commissioners, Hong Kong, 25 – 29 September 2017, https://icdppc.org/wp-content/uploads/2015/02/Resolution-on-data-protection-in-automated-and-connected-vehicles-.pdf

nected cars about upcoming traffic, weather changes, road conditions, and accidents[62].

- Apple has just introduced a **safe driving mode** for the iPhone. The feature ("Do not disturb while driving") prevents owners from receiving messages and calls when driving and lets their contacts know they are occupied. The new feature relies on Bluetooth as the strongest indication that someone is in their car if their iPhone is connected to a car **Bluetooth network**. Moreover, the driving mode uses a number of other signals, such as the iPhone's accelerometer, the rate at which it finds and loses nearby **Wi-Fi networks**, and GPS[63].
- For many years, cars have provided a connection for mechanics and inspectors to measure the electronic functions of the car. Many **maintenance apps** (e.g. Torque[64]) have appeared on the market that allow the On-Board Diagnostics - II (OBD-II) connection to transmit useful stats, such as instant fuel economy, engine speed, temperature, and vehicle speed. These stats are often combined with the accelerometers and GPS locating ability of smartphones. The stats are analysed, and vehicle/journey information is provided to the user on the screen of his or her device.

## 4.2 Challenges imposed by the ePR

### 4.2.1 Wi-Fi and Bluetooth technologies

Both Wi-Fi and Bluetooth tracking are important, if not vital elements in the technological development of connected and autonomous cars. Due to the **abundance of devices** with (open) Wi-Fi and Bluetooth functions and due to more than ten years of research and development of Wi-Fi and Bluetooth based location technology, Wi-Fi and Bluetooth tracking are an obvious option when it comes to the mix of technologies that is presently used in connected and autonomous cars (**"Simultaneous Localization and Mapping - SLAM" technology[65]**).

For the highway stretch in Ohio, **Art. 8 (2) (b) ePR** would require

> *"a clear and prominent notice … informing of, at least, the modalities of the collection, its purpose, the person responsible for it and the other information required un-*

[62] See The Longest Autonomous Car-Ready Highway Nears Completion in Ohio, Inverse Innovation, Aug 2nd, 2017, https://www.inverse.com/article/34830-autonomous-car-highway-ohio.
[63] See How the iPhone's Do Not Disturb While Driving feature works - and how to turn it off, Daily Telegraph, sept., 22nd, 2017, http://www.telegraph.co.uk/technology/0/iphones-do-not-disturb-driving-feature-works-turn/.
[64] See Monitor your car's performance with the Torque app for Android, cnet, July 2nd, 2012, https://www.cnet.com/how-to/monitor-your-cars-performance-with-the-torque-app-for-android/
[65] See Choosing the Best Sensors for a Mobile Robot, Part Two, sensors online, Sept, 29th, 2017, http://www.sensorsmag.com/components/choosing-best-sensors-for-a-mobile-robot-part-two.

*der Article 13 of Regulation (EU) 2016/679 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.*

*The collection of such information shall be conditional on the application of appropriate technical and organisational measures to ensure a level of security appropriate to the risks, as set out in Article 32 of Regulation (EU) 2016/679, have been applied."*

As long as driverless streets are short and few, it may be possible to imagine these streets to be filled with **notice boards** meeting the requirements of Art. 8 (2) (b) ePR. Once there are extensive areas where Wi-Fi and Bluetooth technologies are used, ubiquitous notice boards become hard to imagine. This is especially the case as abundant notice boards can distract drivers and endanger the **safety of traffic**.

Applications like Apple's **safe driving mode** will be hard to operate with the notice requirement of Art. 8 (2) (b) ePR. Art. 8 (2) (b) ePR is modelled on limited spaces like shopping malls where "clear and prominent" notices can, at least, be installed at the entrances. For any car or traffic application, Art. 8 (2) (b) ePR will be understood to mean more than the mere requirement of providing extensive information to the user. Irrespective of the ePR, the app provider must provide such information anyway pursuant to Art. 13 and 14 GDPR. Art. 8 (2) (b) ePR is likely to imply the necessity of installing **permanent "notice boards" in cars** comparable to notice boards at the entrance of shopping malls. This might encourage car companies to install extensive warnings and notices in cars.

### 4.2.2 Car-to-car-communication

Machine-to-machine communication is an essential component of connected car services. Therefore, the car industry would be heavily affected by the ePR as **Recital 12 ePR** explicitly mentions that the ePrivacy Regulation should apply to machine-to-machine communication:

"***Connected devices*** *and machines increasingly communicate with each other by using electronic communications networks (Internet of Things).* […]. *In order to ensure full protection of the rights to privacy and confidentiality of communications* […] *it is necessary to clarify that* ***this Regulation should apply to the transmission of machine-to-machine communications****. Therefore, the principle of confidentiality enshrined in this Regulation should also apply to the transmission of machine-to-machine communications.* […]."

Accordingly, Art. 2 (4) EECC (in connection with Art. 4 (1) (b) ePR) defines an "electronic communications service" as

"[…] *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.*"

The application of the ePR to connected cars would have **fundamental consequences**:

- The ePR protects any content of communication even when there is no information involved that relates to natural or "legal" persons. Consequently, under the ePR, there are no differences between "personal data" and "**machine data**". The standards of protection that the ePR prescribes are strict, and they are fully applicable to "machine data".
- As a rule, Art. 6 ePR requires consent, and in many cases consent is required of the sender of information as well as of the recipient. This means that the development of any application that enables cars or components to communicate would be burdened with the necessity of creating processes that allow for **consent on both ends**. The transmission of signals from a car to a garage for maintenance purposes would require consent of the owner of the garage as well as the driver's consent. Whenever there is a new driver, consent would need to be renewed, and there would need to be a mechanism establishing if a driver is "known" and has already given consent or if there is a "new" driver who still needs to give consent.
- The **abundance of consent requirements** is bound to lead to an abundance of consent requests. Such requests are likely to lead to similar effects as the overuse of cookie banners. They will be perceived by drivers as unwelcome disruptions, and they are unlikely to encourage users to read privacy notices and policies.
- The exact rules of data processing in Art. 6 ePR depend on the distinction between **"content" and "metadata"**. As far as machine-to-machine communication is concerned, there is **only raw** data but no "content" that is transmitted from sender to receiver. When there is no "content", there can, by definition, be no "metadata" as "metadata" is the data processed in connection with the transmission of "content". The lawfulness of processing machine communication data, however, depends on the distinction between "content" and "metadata" according to Art. 6 ePR, although no such distinction is possible, Art. 6 ePR would, therefore, lead to **substantial legal uncertainty** for the whole industry.

### 4.3 Summary

The ePR is likely to be a major burden on the further development of connected and autonomous car technology in Europe:

- **Offline tracking** may well be one of the key technologies in connected and autonomous cars. The use of offline tracking would, however, become highly risky as the strict requirements of Art. 8 (2) (b) ePR would need to be met.
- **Car to car communication** would be subjected to strict privacy rules. The exchange of data between two cars would need to be protected by exactly the same standards as a telephone conversation between two close friends. In order to be on the safe side, car to car communication would often require not only the "sender's" but also the "recipient's" consent. The implementation of consent requests would be a substantial challenge to European carmakers.
- There is **no convincing justification** for the imminent extension of privacy rules to machine data. By definition, machines have no fundamental rights. Moreover, it is, at least, debatable if abundant consent requests are encouraging users to read privacy notices and privacy policies. The experience with cookie banners shows that the overuse of consent requests will often be counter-productive as users will click through such notices without even considering to read privacy information provided.

# 5 General public interest exception ("wiretapping provisions")

## 5.1 Article 11 (1) ePR

Art. 11 (1) ePR allows the EU and its member states to enact exceptions from the provisions of Art. 5 to 8 ePR including for "general public interests":

> "*Union or Member State law may restrict by way of a legislative measure the scope of the obligations and rights provided for in Articles 5 to 8 where such a restriction respects the essence of the fundamental rights and freedoms and is a necessary, appropriate and proportionate measure in a democratic society to* ***safeguard one or more of the general public interests referred to in Article 23(1)(a) to (e) of Regulation (EU) 2016/679*** *or a monitoring, inspection or regulatory function connected to the exercise of official authority for such interests*".

Art. 11 (1) ePR is to replace Art. 15 ePD:

> "*Member States may adopt legislative measures to restrict the scope of the rights and obligations provided for in Article 5, Article 6, Article 8(1), (2), (3) and (4), and Article 9 of this Directive when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system, as referred to in Article 13(1) of Directive 95/46/EC. To this end, Member States may, inter alia, adopt legislative measures providing for the retention of data for a limited period justified on the grounds laid down in this paragraph. All the measures referred to in this paragraph shall be in accordance with the general principles of Community law, including those referred to in Article 6(1) and (2) of the Treaty on European Union*".

Compared to Art. 15 ePD, **Art. 11 (1) ePR lowers the threshold** for EU or member state laws that permit wiretapping or other means of surveillance, including data retention as "general public interests" referred to in Art. 23 (1) (a) to (e) GDPR include, for example (Art. 23 (1) (e) GDPR)

> *"**other important objectives of general public interest** of the Union or of a Member State, in particular an important economic or financial interest of the Union or of a Member State, including monetary, budgetary and taxation a matters, public health and social security"*

**Art. 11 (1) ePR does not set any standards for the restrictions** for the laws that may permit wiretapping or surveillance except for the very general rule that such laws must maintain the essence of fundamental rights and freedoms and be necessary, adequate and proportionate. Furthermore, Art. 11 (1) ePR **ignores** the restrictions on data retention and bulk collection re-

sulting from **the principles that the ECJ set up**[66]. According to the ECJ, no "general and indiscriminate retention of data traffic and location data" is permissible irrespective of the purposes of such retention[67].

### 5.2 Art. 11 (2) ePR

Like Art. 15 (1b) EPD, Art. 11 (2) ePR obliges service providers to co-operate with law enforcement agencies:

> "*Providers of electronic communications services shall establish internal procedures for responding to requests for access to end-users' electronic communications data based on a legislative measure adopted pursuant to paragraph 1. They shall provide the competent supervisory authority, on demand, with information about those procedures, the number of requests received, the legal justification invoked and their response*".

As providers of messenger, webmail, VoIP and other **"over the top (OTT)" services** are now included in the scope of the ePD, this, in fact, means that Art. 11 (2) ePR **silently introduces new obligations** for many providers to co-operate with law enforcement agencies. This clearly contradicts the chief goal of the ePR, which is to protect the privacy of EU citizens.

[66] ECJ Judgement, in case C-203/15 and C-698/15.
[67] ECJ Judgement, in case C-203/15 and C-698/15, point 46.

# 6 Conclusion

The European Commission has drafted a set of rules which aims to provide the necessary flexibility to withstand future technical developments. However, **legal blur** will inevitably lead to legal uncertainty.

For the most part, the draft lacks a clear idea of what technical matters should be regulated and encompassed. This **lack of a clear focus** runs through large parts of the draft. At its core, the draft suggests restrictions on digital services that go far beyond the GDPR and will result in serious risks for the development of the digital economy in Europe.

There is an **open conflict** between **consent requirements** being the strict rule according to the draft ePR and the **more flexible approach in Art. 6 GDPR** that requires consent in some cases but allows also for data processing without consent when such processing is necessary for the performance of a contract or when the service provider can show that he or a third party has legitimate interests that outweigh the interests of data subjects.

The over reliance on consent is based on **false assumptions** when it comes to **legal persons**. The draft aims at protecting privacy and at extending such protection to legal persons. However, it is unclear **whose consent** is relevant. An efficient protection of privacy would mean that the user of a device is the person who needs to give consent. This, however, will always be a natural person whose privacy is already protected by the GDPR. Alternatively, it can be the legal representative of the legal person (company or government agency) who needs to be asked for consent. In privacy terms, this, however means that it is the employer who decides (by giving or refusing) consent about the protection of his or her employees.

The strict consent requirements and **prohibitions** suggested by the draft are, in many cases, not in line with the **users' expectations**. Users expect service providers to "process content" when they pay a provider for his or her services. Users expect their Bluetooth data to be transmitted when they open Bluetooth functions on their devices. They want electronic communications to be secure (an aspect neglected by the draft). At the same time. they want to communicate and often rely on the services of providers for communication. It is a **vital misunderstanding** of the importance of electronic communication as well as of users' expectations when the draft one-sidedly regards digital **communication as a risk and not as a freedom**.

The draft, with all the overlap between the ePR and the GDPR, would lead to legal uncertainty, bureaucratic consent regimes and to an abundance of cookie banners that would make the use of digital services in Europe much less attractive than it now is.

Berlin, 19.10.2017

Prof. Niko Härting

RECHTSANWALT