Committed to Europe

The ePrivacy Draft Regulation

Protecting Privacy in Europe

Background

As a complement to the General Data Protection Regulation (GDPR)[1], on the 10th of January 2017, the European Commission (EC) published a proposal revising the sector-specific ePrivacy Directive (ePD). Unlike the current ePD, the proposed ePrivacy Regulation (ePR) would apply directly across all Member States and would take priority over national legislation. The new ePR significantly expands the scope of the ePD as it would apply to Machine-to-Machine (M2M) communications, certain over-the-top (OTT) communication services[2] - such as communication facilities of travel apps or video games- and to providers situated both inside and outside the EU. The new ePR would reinforce confidentiality of communications; maintain a sector-specific set of rules for processing communication data; and would revise the "cookies rule" that requires websites to get consent from visitors to store or retrieve any information on a computer, smartphone or tablet. Infringing companies would be exposed to fines aligned with the GDPR, of up to €20m or 4% of worldwide annual turnover. Finally, the ePR draft addresses the enforcement of private class actions.

Summary of Orange views

Since the GDPR has significantly strengthened the existing general privacy regime in Europe, maintaining a double set of sector-specific rules for processing data generated through communication services is highly questionable, also in light of the principle of Better Regulation.

Delivering consistent rules for European consumers and companies should, in Orange's views, be the policy-maker's main objective when assessing this new legislative proposal. Orange therefore calls for an alignment with the GDPR and consequent streamlining of double or overlapping provisions:

- Orange calls for a full alignment with the legal grounds for processing metadata under the GDPR – metadata meaning data processed by Electronic Communications Networks (ECN) to transmit communications. Rules for processing personal data should be equal for all, irrespective of the technology used for collection, and not be subject to sector-specific consent rules. In particular, rules applying to the processing of location data should not discriminate between data collected through GPS or electronic communication networks.
- Confidentiality of communications has always been a fundamental principle applied by the telecommunications industry. Orange supports the extension of this fundamental right to any form of interpersonal communications as proposed in the ePR draft. However, concerning machines transmitting personal data, the GDPR already rightly ensures individuals' protection, in a horizontal and technologically neutral way. Machine to Machine communications that do not carry personal data, as in the field of automated supply chains for example, do not justify extensions of individuals' fundamental rights or legitimate interests of legal persons; such communications are rightly covered by the contractual agreements between entities.
- Device data protection is reinforced by several new principles that the GDPR introduced, such as the data minimisation principle, the articles on information duty, and data protection by design and by default. Device data therefore does not need further complex rules that do not fulfil the objective of avoiding over-notification.
- The ePR is presented as a "lex specialis" that "particularises and complements" the GDPR. Nevertheless, the GDPR and the ePR have different scopes, definitions and legal base. Orange considers the ePR overly complex as presently laid out. The following sections explain why and suggest possible solutions.

[1] The General Data Protection Regulation (GDPR) will enter into force in May 2018. The GDPR considerably reinfo rces the level of citizens' protection in terms of information, transparency, possibility to withdraw consent at any time, need for Privacy Impact Assessment and substantial sanctions for infringing companies.

[2] Such as Skype, WhatsApp, Gmail, Facebook Messenger, iMessage, Viber.

Processing of metadata under ePR and of personal data under GDPR should be aligned

EPR defines Electronic Communication Metadata (ECM) as data processed "in an electronic communication network for the purposes of transmitting, distributing or exchanging electronic communications content" such as location data and data used to trace the source or destination of the communication (e.g. call detail records3). On this point, the ePR proposal is not aligned with the GDPR as it does not recognize for example the newly agreed principles of "legitimate purpose" and "compatible further processing". The legal basis to process metadata in the ePR essentially relies on consent. This is unnecessarily restrictive, as requiring hyper frequent consent in the digital area will render consent meaningless, as the current rules for cookies have demonstrated.

Additional improvement is required to the processing of metadata upon users' consent

Under the current ePD, providers of Electronic Communications Services (ECS) can process metadata based upon users' prior consent for direct marketing, or for providing "value-added services" (e.g. traffic information or finding nearby services). Art. 6.2(c) of ePR instead refers to "specific services" while imposing on service providers to ensure that "the purpose concerned could not be fulfilled by processing information that is made anonymous."

Orange welcomes the new wording "specific service" even if this change will have modest impact. On the other hand, Orange considers the obligation to demonstrate that using anonymised data cannot fulfil the same purpose redundant with the data minimisation and privacy by design principles established by the GDPR.

Metadata processing beyond users' consent should be aligned with GDPR rules, including the right to withdraw consent

The processing of metadata beyond users' consent under ePR fundamentally diverges from the GDPR. A justification often quoted for this is that end-users cannot switch off localisation when using telecom services, but it omits the individuals' right to withdraw their consent any time to the processing of location data granted by the GDPR, which gives an appropriate answer to this concern.

Therefore, Orange calls for the full alignment of the ePR with Art. 6 of the GDPR, and specifically:

- Unlike in the proposed ePR, "legitimate interest" and "performance of a contract" are legal grounds for processing personal data in the GDPR. Under this legal basis, the data controller is in charge of assessing the balance between its legitimate interest and the fundamental rights and freedoms of the data subject. The ePR proposal should allow the data controller to perform the same assessment allowed in the GDPR.
- Unlike the ePR, Art. 6.4. of the GDPR states that when the processing is not based on consent, further processing shall be allowed if compatible with the purpose for which the data was initially collected and appropriate safeguards like pseudonymisation have been taken. This is especially important for Big Data analytics, where huge amounts of data from different sources are required, and it is difficult to determine the exact processing purpose at the time of collection.
- Moreover, unlike the ePR, the GDPR has established a strict compatibility test. The controller, after having met all the requirements for the lawfulness of the original processing, has to take into account, inter alia: the context in which the personal data has been collected; the consequences of the intended further processing for data subjects; and the existence of appropriate safeguards, such as pseudonymisation, in both the original and intended further processing operations.

A full alignment of the ePR rules with the GDPR would ensure an effective and consistent protection for users and a workable framework for all providers of services. Policy makers should also avoid setting up rules overwhelming users with consent requests, which are not always efficient, as demonstrated by the "cookie rule" precedent.

Confidentiality of communications is an essential requirement, which is already covered by the GDPR for Machine-to-Machine (M2M) communications

The new ePR revises both the rule and the scope of confidentiality of communications:

- The new rule requires deletion or anonymisation of records as soon as the communication has been terminated, unless there is a specific justification to retain such data (see ePR Art. 7.2). Valid justifications are billing, quality control to fulfil obligations, cybersecurity or prior consent provided by the end-user.
- All providers of ECS and ancillary services are now within the scope of the obligations, including M2M communications.

[3] A Call Detail Record may contain times, origins and destinations of phone calls, electronic messages, instant messages and other modes of telecommunication, as opposed to the content of the message itself.

Orange agrees with the view that confidentiality is now the responsibility of all interpersonal communications providers and supports this extension. However, Orange disagrees with the explicit reference to M2M communications that is questionable on many aspects:

- According to recital 12, the ePR would apply to any "connected device and machine that increasingly communicates by using electronic communication networks (Internet of Things)", but "connected devices and machines" are not defined, nor their relation to the "terminal equipment"4 which is the limit of telecom operators' liability;
- As nearly all digital machines communicate, any legal and natural person that are owners of any connected devices or machines should express consent according to the ePR rules for the processing of electronic communication data for both personal and non-personal data;
- M2M connectivity is broadly defined in recital 14 encompassing the connectivity provided as ECN[5], which means by telecom operators. For example, end-users that would choose to connect their vehicles through an ECN would receive a reminder of the possibility to withdraw consent every six months. This would not be the case with others "non-ECN" connectivity, i.e. Vehicle-to-Vehicle or Vehicle-to-Infrastructure systems.

Following the "lex specialis" rule, the ePR will prime over the GDPR on those issues and impact the whole digital economy as it goes beyond protecting confidentiality of communications and considerably limits the processing of data. Orange considers that the GDPR is the appropriate tool to protect individuals' personal data carried by M2M communications services6. The legitimate interests of legal persons are better protected by the terms and conditions foreseen in business contracts that are the relevant instruments to deal with this topic. M2M communications should thus be excluded from the scope of the ePR. Moreover, the ePR should focus on personal data and the extension to non-personal data is not justified. Finally, as telecom operators cannot be held liable for any device communicating beyond the terminal equipment, it should be clear that the ePR does not cover communication networks beyond ECN as for example over Near Field Communication or Bluetooth.

Other changes to reduce complexity are required

In Orange views, the ePR proposal requires a substantial simplification on many aspects, also to ensure smooth implementation; this can be done without lowering the level of protection.

Extension to non-personal data is unclear and questionable

The ePR proposal is based on new definitions. Electronic Communication Data (ECD) covers both Electronic Communication Content (ECC) - the content exchanged by means of ECS, such as text, voice, videos, images and sound – and ECM, which means metadata as explained before.

As opposed to the current ePD[7], Art. 2(1) of ePR establishes that the regulation "applies to the processing of ECD carried out in connection with the provision and the use of ECS and to information related to the terminal equipment of end-users". Recital 4 of the ePR confirms that "ECD may include personal data as defined in the GDPR." This would mean that ECD may also include non-personal data. Two cases may arise:

- ECD is personal data: the GDPR applies by default, and the ePR will be lex specialis, meaning it will prevail when the two regulations establish rules for the same situation. However, Recital 5 of the ePR explains that the ePR should not lower the level of protection enjoyed by natural persons under the GDPR.
- ECD is not personal data: e.g. information related to the terminal equipment that does not belong to the end-users. In this case the ePR would apply, but not the GDPR. The legal base for this extension to non-personal data and the interactions of this proposal with other legislative initiatives (i.e. Free Flow of Data) aiming at potentially regulating non-personal data are unclear.

---

[4] Terminal equipment is defined by Directive 2008/63/EC

[5] Connectivity needed for IoT and M2M does not only rely on ECN. Common examples of Personal Area Network (PAN) are the Ethernet and the Powerline. Examples of short range wireless connectivity solutions include: Near Field Communication (NFC), Radio Frequency Identification (RFID), Infra-Red (IR), Bluetooth, local Wi-Fi and license free networks as Sigfox, LoRa, V2V, etc.

[6] IoT and M2M services carrying personal data will be subject to the following GDPR's articles: lawfulness of processing (Art. 6) with the new definition of consent, the security notification regime (Art. 33 and 34), privacy by design and privacy by default (Art. 25), data minimization (Art. 5.1c) and also to the enhanced data subjects rights as: the right to be forgotten (Art. 17), the right to data portability (Art. 20), the right to object to automated decision making (Art. 22), rights of children (Art. 8).

[7] The current regime of the ePrivacy Directive is centred on the processing of personal data (see Art Article 3(1) of Directive 2002/58).

Extension of consent requirement to legal persons can create implementation issues

The GDPR covers individuals and the ePD covers individuals using ECS for personal and business purposes. The new ePR also covers both natural and legal persons, but unlike the ePD, Recital 3 of the ePR extends the duty to collect consent to legal persons without describing how this new principle should be implemented and how this new consent of legal persons relates to the consent of natural persons.

Rules for processing location data diverge from GDPR and discriminate providers

Recital 17 of the ePR explains that "location data generated other than in the context of providing ECS should not be considered as metadata". This exposes consumers and individuals to a double set of rules depending on the "context" of the provided service and irrespective of the objective criteria based on the degree of sensitivity of a particular type of personal data or the precision of a specific technology.

In other words, a similar location service would be ruled differently depending on its underlying technology: electronic communication networks or GPS. For instance, non-communication "apps" revealing how long individuals stay in a shop, or even how long consumers look at merchandise before buying it, would only be regulated by the GDPR. There is no justification to make such a distinction, especially considering that information retrieved from networks can be less precise than those obtained via GPS for instance. As showed by recent studies[8], delivering consistent rules for European consumers should be the main objective of regulators.

Orange considers ePR far too complex in this matter and calls for a true alignment with the GDPR. The ePR should be driven by the objective to provide identical privacy protection to consumers, whichever service provider they choose, and identical opportunities to all providers of digital services to develop data based innovations.

Changes on consent to cookies do not fulfil the objective to avoid over-notification and carry risks for competition

Under the ePR, "software permitting electronic communications" including browsers would require users, when they install the software, to choose whether they want to prevent third parties from gaining access to the information on their device. The choice made by users would be enforceable against all third parties.

The new ePR does not avoid over-notification from websites, as those whose business models are based on audience will need consent banners to inform individuals that they can change their settings to access their service. Orange considers that GDPR reinforces the protection of device data and that the ePR should not introduce further complex new rules. Specifically, the data minimization principle, Articles 12 to 14 of GDPR on information duty, and data protection by design and by default are all appropriate tools to protect device data.

Furthermore, the distinction made by the text between "first-party" cookies and third-party cookies does not bring more security to end users' privacy: it is the purpose of the cookie that matters and is likely to impact privacy. Moreover, by giving a pivotal role to software companies such as providers of Internet browsers, several of which also carry Internet services and advertising activities, the new ePR could severely harm competition. The draft regulation does not include any guarantee for non-discrimination in relation to software providers' own services. Generally speaking, the current wording gives a significant strategic advantage to vertical, integrated, identification-based ecosystems and does not seem to take into account business models based on advertising and targeting, that are increasingly essential to the very functioning of the Internet (e.g. recommendation tools).

Finally, the draft ePR proposes to protect end-users from unsolicited direct marketing communications, the definition of which is unclear and may include behavioural on-line advertising. Once more, the ePR therefore risks conflicting with existing provisions in the GDPR, as well as with provisions of the Open Internet Regulation that prohibit electronic communications providers from blocking ads even at end-users' request. Clarification is required.

For more information: https://oran.ge/in-Brussels , or follow us on Twitter: @Orange_Brussels

---

[8] A survey commissioned by ETNO in 2015 ([8] http://www.comresglobal.com/polls/etno-digital-consumer-survey/) demonstrates that consumers do not fully understand the current protection standards over the use of their personal data, for example whether they are localised by GPS or by telecommunication networks. The research shows that 7 in 8 respondents (88%) are not aware of the higher levels of data protection when using regulated telecom services as opposed to online services. An independent study carried out by the Commission also highlights the inconsistencies of the double regulatory regime for the telecommunication. See SMART 2013/0071, June 2015, p 9 : "It is difficult to justify why traffic or location data should receive different legal protection if they are processed in the context of very similar services from a functional perspective."