First Wave of Ripple Effects of the General Data Protection Regulation

By Alex van der Wolk and Sotirios Petrovas
Morrison & Foerster

As part of the Digital Single Market (DSM) strategy outlined in May 2015, the European Commission (the “Commission”) issued a communication and two proposals in early January to further enhance and update the legal regime for data protection in the Union.

The Commission issued:

• a Proposal for a new “ePrivacy” regulation to replace the current directive of 2002 on privacy in the sector of electronic communications¹

• a Proposal for a new regulation governing data protection rules for EU institutions,² and

• a Communication to Parliament and Council on the cross border data transfers instruments to countries outside the EU and the framework for recognizing foreign jurisdictions as “adequate.”³

The objective of these initiatives is to build on the momentum created by the adoption of the General Data Protection Regulation (Regulation (EU) 679/2016 or “GDPR”) and to bring the entire constellation of EU data protection instruments up to par with the standards it sets. The GDPR was adopted last April after four years of legislative debate and is set to take effect in May 2018.

PROPOSAL FOR A NEW EPRIVACY REGULATION

The Commission issued its proposal for a new regulation concerning the respect for private life and the protection of personal data in electronic communications (the “ePrivacy Regulation”) on January 10, 2017, marking the official start of the legislative process for its negotiation and ultimate adoption by Council and Parliament.

Once adopted, the new ePrivacy Regulation will repeal the current ePrivacy Directive 2002/58/EC (the “ePrivacy Directive”) and prevail over any contrary provisions of national legislation adopted pursuant to the ePrivacy Directive.

Overall, the principles as included in the ePrivacy Directive remain largely unchanged. Being a regulation, however, the new instrument will have direct effect and will be immediately applicable in all Member States.

The purpose of this choice is to ensure greater harmonization and consistency of ePrivacy rules in the Union and to reduce burdens for business to operate cross-border. The following is an overview of the proposed ePrivacy Regulation’s key features.

Scope

The ePrivacy Regulation includes rules on the processing of electronic communications data that are mainly addressed to:
The Regulation also includes substantive rules on the use of cookies and similar tracking technologies, as well as rules on direct marketing, which apply to all companies (Recital 8).

It is important to also note that the ePrivacy Directive and the upcoming ePrivacy Regulation are part of the broader regulatory framework for electronic communications, which is currently subject to ongoing revision.

The Commission proposed in September 2016 a draft directive establishing the European Electronic Communications Code (“EECC”), and many definitions in the ePrivacy Regulation explicitly refer to the EECC.

**Rules for providers of electronic communication services**

The ePrivacy Regulation has a number of provisions for the processing of electronic communications data, including content data and metadata, that apply to telecommunication providers only.

Because the Commission considers that the objectives and principles of the current ePrivacy Directive are still appropriate and relevant, the rules essentially remain unchanged in substance.

What will change, however, is that the new ePrivacy Regulation will be extended to also apply to providers of internet-based services enabling interpersonal communications such as VoIP, instant messaging, and web-based email, collectively called “Over-the-Top communications ("OTT") services.

As a result, the rules will now also apply to social media that offer instant messaging and chat functionalities, email providers, and VoIP service providers.

The change in scope is effectuated by a broadening of the definition of “electronic communications services” in the EECC, which also includes “interpersonal communications services” (emphasis added).

Interpersonal communications services are Services “that enable 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).”

**Cookies and information stored on users’ terminal equipment**

The requirements for the use of cookies are maintained, but the wording is changed with the aim to be more technologically neutral and to thus capture similar technologies (e.g., device finger-printing).

According to Article 8(1), 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” is only permitted in four circumstances:

- if it is necessary for the sole purpose of carrying out the transmission of an electronic communication over an electronic communications network;
- if the end-user has given consent;
- if it is necessary for providing an information society service (as defined by Directive (EU) 2015/1535) requested by the end-user; or
- if it is necessary for web audience measuring (provided this is carried out by the website owner — the provider of the information society service requested by the end-user).

These requirements largely reflect the general rules laid down by Article 5(3) of the current Directive and the implementation of the Directive in Member States’ implementing legislation.
What is new, however, is the exemption for website analytics, which — according to the recitals — should be possible on condition that their use has very little or no impact on end-users’ privacy and is carried out by the owner of the website to which the analytics pertain (which would suggest it pertains to first party analytics only).

Finally, Article 8(2) also limits the collection of “information emitted by terminal equipment to enable it to connect to another device and/or to network equipment” (emphasis added).

This would cover for example Wi-Fi, beacon scanning or other location-based tracking (see Recital 25). The ePrivacy Regulation acknowledges that such emitted information may be used for functional purposes (such as assessing the number of people waiting in line or the total number of people in a given area) but also for commercial purposes (such as proximity marketing).

The Regulation provides for limitations on the collection of such information, which is only permitted:

- if it is done exclusively for purposes of establishing a connection (i.e., a technical purpose); or
- upon the display of a clear and prominent notice (prior to entering the defined area) and the purpose of the tracking, as well as information on how the user can stop or minimize (i.e., reduce) such collection.

If the information collected also qualifies as personal information, then the information requirements under the GDPR (also) apply. In addition, the entity collecting such data must implement appropriate security, as required under GDPR Article 32.

It is interesting to note here that, for capturing information emitted by devices, a notice suffices, whereas capturing information online (e.g., cookies) is subject to consent. A previous (leaked) draft of the ePrivacy Regulation (December 2016) had also suggested an opt-in requirement for capturing emitted information, but that has not been maintained in the current proposal.

**Consent**

With regard to consent requirements, Article 9(1) of the ePrivacy Regulation explicitly references the GDPR. Consent must thus be “freely given, specific, informed and unambiguous” and amount to a “statement or a clear affirmative action” signifying his or her agreement, and the same conditions apply as in GDPR Article 7 (including, for example, the possibility to easily withdraw consent at any time).

Interestingly, Article 9(2) of the ePrivacy Regulation provides that, where technically possible and feasible, in the context of cookies and similar technologies covered by Article 8(1) of the ePrivacy Regulation, consent may be expressed via the settings of the browser or internet navigation software, provided browsers are set up to facilitate a clear and affirmative action signifying the acceptance of cookies (i.e. not accept all cookies by default — see also below on Privacy by Default).

Furthermore, the recitals indicate that the methods for obtaining consent should be “as user-friendly as possible” and transparent (Recital 22) and that opt-in consent should be obtained for the storage of third-party tracking cookies (Recital 24).

**Privacy by default requirement: Less strict requirements in final draft**

In a previous (leaked) draft version of the ePrivacy Regulation, Article 10 provided for a general privacy-by-default rule according to which browsers and software should be configured in such a way that their settings should by default “prevent third parties from storing information, processing information already stored in the terminal equipment and preventing the use by third parties of the equipment’s processing capabilities.”

In the published, final proposal for the ePrivacy Regulation, this provision has been significantly watered down to a standard that is much less strict: such browsers/software must now merely (1) “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” and (2), upon...
installation, “inform the end-user about the privacy settings options and, to continue with the installation, require the end-user to consent to a setting.”

**Direct marketing**

Under the draft ePrivacy Regulation, the rules for direct marketing also remain largely unchanged, with the biggest effect that — by virtue of the instrument being a regulation — they will be harmonized throughout the Union: Article 16(1) provides that consent is required for sending marketing messages via electronic communication services.

It is interesting to note that, in the context of direct marketing, the language of the ePrivacy Regulation marks a significant departure from the ePrivacy Directive.

Whereas the latter was confined to the use of “automated calling systems without human intervention (automatic calling machines), facsimile machines (fax) or electronic mail” (emphasis added) for purposes of direct marketing (article 13 of the Directive), the new ePrivacy Regulation refers to the more generic term “electronic communications services” (at Article 16(1)) (emphasis added). As indicated above, this will now also include “interpersonal communications services,” which may possibly affect a broader range of communication channels.

Another notable change is that the consent requirements for direct marketing under the ePrivacy Regulation apply to natural persons only. The draft Regulation explicitly leaves it to Member States to address B2B marketing (Article 16(5)).

The “soft opt-in exception” provided for in the current ePrivacy Directive (at Article 13(2)) is maintained.

Consent is therefore not required if an entity sends direct marketing communications to customers of whom it obtained the contact details in the context of the sale of a product or service, provided such communication pertains to the company’s own similar products or services and an opt-out is offered at the time of collection and in each communication.

The ePrivacy Regulation gives the possibility to Member States to allow voice-to-voice direct marketing calls (i.e., that do not make use of automated means) on the basis of opt-out.

**Penalties**

A big change is that the regime for penalties is aligned with the GDPR (Article 23 contains an explicit reference to Chapter VII of the GDPR). Thus, fines may reach up to 4% of a company’s total worldwide annual turnover or 20 million euros (whichever is higher).

The maximum amounts are, however, reserved for violations of some telecommunications obligations. The requirements pertaining to “cookies,” “emitted information,” and direct marketing are subject to the 2%/10 million euro maximum.

**Next steps**

The issuance of the Commission’s proposal officially marks the beginning of the legislative process. The Commission invited Council and Parliament to ensure adoption and effective entry into force of the ePrivacy Regulation by 25 May 2018, which is the date of entry into force of the GDPR.

**COMMUNICATION ON CROSS BORDER TRANSFERS AND ADEQUACY DECISIONS**

The Commission issued a Communication describing a strategic approach on the issue of cross border transfers of personal data and issuing adequacy decisions to non-EU jurisdictions.

The Commission expressed its intention to conduct discussions with “key trading partners” that guarantee an “essentially equivalent” level of data protection in their legislation to reach “Adequacy Decisions” to allow the unfettered transfer of personal data such countries.

The criteria for deciding which countries to start a dialogue on adequacy will include:

- the extent of commercial relations with the EU,
- the extent of personal data flows from the EU,
• the “pioneering role” of the country in the field of privacy and data protection in its region, and
• the overall political relationship, in particular with respect to promoting common values and shared objectives at international level.

Discussions on adequacy status will most noticeably concern countries in East Asia, Latin America, and certain countries of North Africa, the Middle East, and the Black Sea (i.e., the “European Neighborhood” countries).

India may also be concerned, depending on its “progress towards modernizing its data protection laws.” The Commission indicated that it is already planning to start negotiations with South Korea and Japan in the course of 2017.

Assessing a country’s adequacy requires both a review of substantive protections applicable to personal data and the applicable oversight and redress mechanisms effectively in place. The list of countries currently recognized as offering an adequate level of data protection is available online.\(^6\)

For countries that do not relish “adequacy” status, the Commission declared that it will make full use of other available tools under the new data protection regime to facilitate the exchange of personal data.

This includes, for example, cooperation in the framework of the Police Directive and the Umbrella Agreement concluded with the U.S. It is of particular interest that the Commission also mentions the possibility to put in place sector-specific Standard Contractual Clauses (SCCs), and even processor-to-processor SCCs, bearing in mind that such tools do not currently exist.

Finally, the Communication outlines the Commission’s strategy for promoting international data protection standards, including through multilateral instruments. In particular, the Commission will encourage countries to accede to the Council of Europe Convention 108 and its additional Protocol.

Despite it being originally a Council of Europe instrument, Convention 108 is open to accession to countries that are not Council of Europe member states. In fact, countries such as Uruguay and Senegal have ratified the convention.

The Commission will also engage with important new actors, such as the United Nations Special Rapporteur on the Right to Privacy to promote data protection at the international level.

**PROPOSAL FOR A NEW DATA PROTECTION REGULATION ON DATA PROTECTION RULES FOR EU INSTITUTIONS AND BODIES**

The data protection rules that apply to EU institutions and bodies are currently governed by Regulation EC No. 45/2001, and the European Data Protection Supervisor (EDPS) is responsible for controlling their implementation.

To align these rules with the GDPR, the Commission has proposed a new draft Regulation to Parliament and Council.

The new data protection regime will essentially cover the processing of employees of the EU institutions and bodies, visitors, and NGOs or businesses that receive EU funding.

In summary, key changes include:

• enhanced transparency and rights for individuals: use of clear and plain language in privacy statements, a right to erasure (or “to be forgotten”), in particular where personal data is no longer needed and the individual objects or withdraws consent, and a right to portability;
• consent must be obtained in the same manner as dictated by the GDPR (i.e., using clear and plain language, avoiding “bundled” consent, and allowing withdrawal of consent at any time);
• institutions and bodies must notify data breaches to the European Data Protection Supervisor (EDPS) and, in some circumstances, to affected individuals;
• simplified, less bureaucratic procedures;
• the EDPS will be empowered to impose fines for violations of data protection rules; and
• data protection by design and by default and impact assessments.

The ultimate goal of this overhaul of EU legislation is to set the foundations for the growth of an EU-wide digital economy, one of the DSM strategy’s top priorities.

Businesses should closely follow the discussions on ePrivacy and cross border transfers and start making preliminary assessments on how these changes may impact their operations. The new instruments and initiatives are set to be effective by 25 May 2018, which leaves little room for hesitation.

NOTES


4 Additional information on this draft directive can be found online at http://bit.ly/2lhEwvn.

5 The current draft of the EECC is available online at http://bit.ly/2caAmrr.

6 The list of countries currently recognized as offering an adequate level of data protection is available online at http://bit.ly/2fSMoXN.