

On 10 January 2017, the EU Commission published a [proposal](#) for a new regulation on e-Privacy (ePR).<sup>1</sup>

The ePR is intended to replace the current e-privacy Directive (ePD), updating it in line with the General Data Protection Regulation (GDPR) and technological developments that have occurred since the last amendment of the ePD in 2009. By proposing to convert the directive into a regulation, the ePR, if adopted, will not need to be transposed into national law and will have direct effect in all EU Member States. The European Commission thus aims to achieve a higher level of harmonisation in the e-privacy arena although; the proposed ePR still allows Member States to adopt national rules in a few areas.

Like the existing directive, the draft ePR contains rules specifically applicable to providers of electronic communications networks and services, as well as rules of a general application. The ePR is intended to complement the GDPR and will take precedence when the ePR rules apply.

## Rules Applicable to Electronic Communications

The definition of an electronic communications service would be expanded to include online services beyond traditional electronic communications voice and data services, including Voice over IP, messaging services and web-based email services. This is in line with the definitions contained in the proposed Electronic Communications Code (ECC), which is currently being debated by the EU Parliament and Council. By contrast with the ECC, the definition of “electronic communications service” under the ePR will additionally include ancillary electronic communications services linked to another service, e.g. messaging services that are embedded in dating apps and video game services.

Similar to the GDPR, the ePR will be extended to cover electronic communications service providers not established in the EU that provide services to end-users in the EU, including both natural and legal persons. Such providers will have to designate a representative in at least one EU Member State.

The ePR maintains the principle of the confidentiality of electronic communications data and sets out the conditions under which such information may be processed. The proposed definition of electronic communications data includes content (i.e. text, voice, videos, images and sound) and metadata (i.e. data required for the purposes of transmitting, distributing or exchanging content, such as numbers called, the websites visited, geographical location, the time, date and duration when an individual made a call, etc.).

The ePR proposes to apply this principle to the transmission of machine-to-machine communications underlying the Internet of Things as well.

Further provisions deal with the storage and erasure of electronic communications data. End-users’ consent features prominently as one of the conditions for permitting processing under the ePR. The stricter rules on consent that apply generally under the GDPR would also apply to electronic communications.

## Rules of General Applicability

As in the current ePD, certain key provisions of the ePR will apply generally and not just to electronic communications service providers. These concern the protection of access to, and the information stored in, end-users’ terminal equipment (essentially an amended “cookie provision”) and the sending of unsolicited communications (spam).

### Cookies

The “cookie provision” under the ePD has been modified in the proposed ePR to cover a wider array of cookie-like applications that use the processing or storage capabilities of an end-user’s device. The end-user’s prior consent remains the key basis for allowing the use of those capabilities except in very limited circumstances. As mentioned above, the provision of, and the conditions for obtaining, consent are defined in the draft ePR by explicit reference to the GDPR, but consent may also be expressed by using the appropriate technical settings of a browser through transparent and user-friendly settings. There is also a new provision regulating the collection of information emitted by terminal equipment.

Another new requirement under the proposed ePR is that all software placed on the market which permits electronic communications, including the retrieval and presentation of information on the internet, would need to offer users the option to prevent third parties from storing or processing information (e.g. cookies) on the user’s terminal equipment. The software would have to inform end-users about the privacy settings and require their consent to a particular setting. These settings would be set when the browser is installed<sup>2</sup> and would then apply to all the websites the user views using the software. For example, a user would be able to choose between never accepting cookies, rejecting third-party cookies and only accepting first-party cookies.

<sup>1</sup> At the same time, the Commission issued two communications on “[building a European data economy](#)” and “[towards a thriving data-driven economy](#)”.

<sup>2</sup> Where software is already installed, the requirement to choose these privacy setting must be provided when the software is next updated, but by no later than 25 August 2018.

## Spam

The provisions of the ePR that relate to spam propose to expand the current limitations of the ePD to prohibit all types of unsolicited communications (including via SMS, MMS and Bluetooth) without the recipient's prior consent. The extended scope would also cover direct marketing phone calls, but the ePR would allow EU Member States to use a system that allows users to register on a "do-not-call list" instead. The exception contained in the ePD for pre-existing customers would remain but would be further refined.

## Enforcement

The draft ePD contains a proposal that would make the national supervisory authorities responsible for monitoring compliance with the GDPR responsible for monitoring the application of the ePR as well (rather than the supervisory bodies for electronic communications). Among other things, the supervisory authorities would be empowered to impose administrative fines of up to 4% of total worldwide annual turnover, reflecting the maximum GDPR fines.

## Next Steps

The proposal will now be reviewed by the European Parliament and Council. The EU Commission has proposed the adoption of the ePR in time for it to come into force on 25 May 2018, the date on which the GDPR will become enforceable. This is an ambitious objective given the range of concerns that both industry and consumer rights groups have already voiced with regard to various provisions of the draft ePR.

## Contacts

### **Ann LaFrance**

Partner, London  
T +44 207 655 1752  
E [ann.lafrance@squirepb.com](mailto:ann.lafrance@squirepb.com)

### **Monika Kuschewsky**

Partner, Brussels  
T +322 627 76 46  
E [monika.kuschewsky@squirepb.com](mailto:monika.kuschewsky@squirepb.com)

### **Matthew Buckwell**

Associate, London  
T +44 207 655 1276  
E [matthew.buckwell@squirepb.com](mailto:matthew.buckwell@squirepb.com)