GOWLING WLG

EUROPEAN EPRIVACY REGULATION: WHAT NON-EUROPEAN COMPANIES NEED TO KNOW

31 May 2018

Articles

Later this year, Europe's ePrivacy Regulation will likely to come into effect, repealing the current ePrivacy Directive and serving as a *lex specialis* to the General Data Protection Regulation ("**GDPR**"). The regulations will cover the processing of personal data and the protection of privacy in the electronic communications sector.

Once in force, the ePrivacy Regulation like the GDPR will apply in the 28 Member States of the European Union ("**EU**") as well as, through mirroring legislation, in Norway, Iceland and Liechtenstein (combined, the European Economic Area or "**EEA**").

North American and other non-European companies that have had to determine whether or not they will fall within the territorial scope of the GDPR, will have to repeat the same exercise with the ePrivacy Regulation.

Below, are some key details about the ePrivacy Regulation to help non-European companies make that determination.

IS IT CONCEIVABLE THAT THE EPRIVACY REGULATION APPLY TO A NON-EUROPEAN COMPANY THAT FALLS OUTSIDE THE TERRITORIAL SCOPE OF THE GDPR?

Given the potentially larger territorial scope of the ePrivacy Regulation, it is conceivable that the ePrivacy Regulation could apply to non-European companies that fall outside the territorial scope of the GDPR.

Indeed, the latest draft of the ePrivacy Regulation at the time of writing this article purports to apply to all areas where individual end-users in the EU are involved. The GDPR, conversely, will only apply to persons (including companies) established outside the EU (or EEA) insofar as they carry out **processing activities** in respect of personal data of individuals within the EU (or EEA). Further, under the GDPR, these activities must be related to the offering of goods or services or the monitoring of behaviour, whereas the proposed ePrivacy Regulation makes no such stipulation.

A non-European company falling into such an unlikely situation would have to comply with the specific notice, consent and other requirements set out in the ePrivacy Regulation, including the obligation to appoint a representative in the EU, but not, say, the obligation to maintain a record of processing activities under article 30 of the GDPR.

Such a situation, however, would not fit well with the ePrivacy Regulation's stated aim to "particularise and complement the general rules on the protection of personal data" laid down in the GDPR.

Some companies may therefore take the view that if they fall within the scope of the ePrivacy Regulation, they must necessarily fall within the scope of the GDPR, even if it means adopting a liberal interpretation of the notions of "offering of goods and services" and "monitoring."

WHAT ARE THE AREAS COVERED BY THE E-PRIVACY REGULATION?

According to its latest draft, the ePrivacy Regulation will have a larger scope than the European ePrivacy Directive of 2002 (as amended in 2009) it will replace, covering:

- the processing of electronic communications data (content in transmission and metadata) of end-users who are in the EU, carried out "in connection with the provision and the use of electronic communications services";
- cookies and more generally information processed by or emitted by or stored in the terminal equipment of end-users who are in the EU;
- the placing on the EU market of browsers and other software permitting electronic communications, including the retrieval and presentation of information on the internet;
- the offering of a publicly available directory of end-users of electronic communications services who are in the EU;
- the sending or presenting of direct marketing communications to end-users who are in the EU.

We shall focus hereafter on the first (processing of electronic communications data), second (cookies) and last (direct marketing) of the above-listed areas because of their potentially large impact.

Processing of electronic communications data

The ePrivacy Regulation will primarily apply to providers of electronic communications services, including providers of internet access, hotspots, voice over IP (VoIP) as well as connected devices and software-based applications for smartphones (where there is provision of transmission services used for the provision of machine-to-machine services involving the conveyance of signals via an electronic communications network). It will contain specific provisions requiring them to seek consent from end-users for an array of purposes.

The language used in the draft ePrivacy Regulation suggests it could apply not only to the provision of electronic communications services but also to their "use" if it involves interfering with - or more generally processing - the (content or metadata) data being transmitted.

For instance, a company that merely publishes a website or app would not in itself constitute a provider of electronic communications services. However, if it publishes ads on its website or app or emails containing web beacons allowing content to be downloaded from the server of the advertiser and in the process allowing the latter to collect the Internet Protocol (IP) address, device information and the value of browser identifier cookies (enabling the advertiser to keep a time log of the webpages and emails viewed by the same browser or the same IP address), the question then arises whether this would entail processing electronic communications metadata "in connection with the provision and the use of electronic communications services."

The draft goes on to prohibit any interference with - and more generally any processing of - electronic communications data, except where permitted by a specific provision in the regulation. Despite this exception, the only provisions permitting such interference in the current draft are addressed to providers (not users) of electronic communications services, essentially requiring them to seek the consent of the end-user except in limited cases. Hopefully this will be clarified in the final version of the text.

Cookies

The ePrivacy Regulation will maintain the existing requirement (under the E-Privacy Directive) that the consent of end-users shall be obtained before installing certain cookies on their terminals, while potentially exempting audience measuring and security update cookies under certain conditions. This regime will be extended to, more generally, the collection of information from an end-users' terminal equipment, including through "web bugs" (another name for web beacons) according to the recitals.

It is unclear yet if it will be possible to continue obtaining implied consent through a cookie banner or if some express consent will be required (without prejudice to the possibility for end-users to refuse consent through the settings of their browsers pursuant to the new requirements for browsers marketed in the EU under the draft regulation). Some additional information on the modalities of collection may need to be included in the cookie notice.

Direct marketing

The ePrivacy Regulation will likely confirm the existing requirement (under the E-Privacy Directive) that the (opt-in) consent of end-users who are natural persons shall be required in order to send them direct

the (opt-in) consent of end-users who are natural persons shall be required in order to send them direct marketing electronic communications. Communications concerning products or services similar to those sold by the same entity to the relevant end-user would be excepted from this requirement, provided that end-users have been given the opportunity to opt-out at the time of collection and each time they receive a communication.

These rules will also apply to the "presenting" of direct marketing electronic communications, such as ads on a website or app that are directed to a specific identified or identified end-user.

The recitals indicate that these rules will apply not only to businesses but also to political parties and other non-profit organizations (whereas European countries had divergent interpretations as regards the application of the relevant rules of the E-Privacy Directive to non-profit organizations).

Opt-in consent will not be required, however, for emailing legal persons (though it will be possibly required for emailing unincorporated businesses since they are, strictly speaking, end-users who are natural persons), nor will it be required for non-automated voice-to-voice calls (subject to specific legislation in each country) or solicitation by regular mail. The processing of personal data for direct marketing purposes in such circumstances could be regarded as lawfully carried out for a legitimate interest, as put in the recitals of the GDPR, and be subject to the rights of objection and erasure set out therein (at least when individuals are concerned).

DO I NEED TO APPOINTMENT A REPRESENTATIVE IN THE EU?

According to its latest draft, the E-Privacy Regulation will also require specific entities to designate in writing a representative in the EU when they are not established in the EU themselves. This will apply to:

- providers of electronic communications services to end-users who are in the EU;
- persons using electronic communications services to send or present direct marketing communications to end-users who are in the EU; and
- persons making use of processing and storage capabilities or collecting information processed by or emitted by or stored in the terminal equipment of end-users who are in the EU.

WHAT ARE THE PENALTIES FOR NON-COMPLIANCE?

Violation of the E-Privacy Regulation could result in administrative penalties up to €20 million or, in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher (as the term undertaking is used in articles 101 and 102 of the Treaty on the Functioning of the EU, namely with reference to relevant economic activity, not the relevant legal entity). They may also be held civilly liable for damages caused by non-compliance or face criminal penalties.

Related Privacy & Data Protection, General Data Protection Regulation

AUTHOR

Danhoé Reddy-Girard

Partner

Paris
T:+33 (0)1 42 99 35 45
danhoe.reddy-girard@gowlingwlg.com

View profile

RELATED INSIGHTS & RESOURCES

New Mandatory Breach Reporting under the Alberta Health Information Act

Krista Schofer

Articles 18 Jun 2018

Are you compliant with the new EU General Data Protection Regulation?

Danhoé Reddy-Girard

Articles 16 Apr 2018

PIPEDA data breach reporting to take effect November 1, 2018

Joshua Shoemaker, Wendy J. Wagner, Naïm Alexandre Antaki

Articles 05 Apr 2018

View all