

Proposed EU E-Privacy Regulation

Date : February 16, 2017

These FAQs answer some basic questions about the proposed EU E-Privacy Regulation. For an explanation of various data protection terms and concepts please consult our EU General Data Protection Regulation (“GDPR”) glossary [here](#). If you would like detailed advice on the proposed E-Privacy Regulation we are happy to help - our contact details are at the end of these FAQs.

What is this all about ?

At the start of January 2017 the EU issued a legislative proposal to upgrade existing privacy rules in electronic communications, notably to be aligned with the GDPR (see [here](#) for our GDPR FAQs). The proposed revised rules are called “Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)” (“E-Privacy Regulation”), which can be found [here](#).

What format will the proposed new rules take ?

The existing E-Privacy rules are in the form of an EU Directive that the EU Member States had to implement into their national legislation. The proposed new rules are in the form of a Regulation meaning that it will be uniformly applied (although national law may flesh out some aspects in further detail, e.g see below about marketing calls), and, once the proposed E-Privacy Regulation has been adopted by the EU it will automatically become national law in the Member States.

Who does this apply to ?

The proposed E-Privacy Regulation will cover a wider scope of providers than under the current rules. In addition to traditional telecoms service providers, other providers of electronic communications services will also be included (irrespective of whether a payment from an end-user is required or not). Therefore, providers such as Whatsapp, Facebook Messenger, Skype, Gmail, Viber etc will fall under its scope.

Do the proposed new rules also apply to service providers based outside the EU ?

Yes. Where a service provider is not established in the EU it will have to designate a representative in the EU, who will be established in the EU Member State where the end-users of the electronic communications are located.

What about consent ?

Consent runs through much of the proposed E-Privacy Regulation and it will have to be freely given - the definition of and conditions for consent will be the same as under GDPR (see our GDPR FAQs [here](#) for more on this).

What content will be covered ?

The scope of the proposed E-Privacy Regulation covers all electronic communications data, i.e it is not limited to “personal data” but covers data related to an end-user (individuals and entities). Both more traditional content (text, voice, video, images, sound etc) and metadata (data used to trace source and/or location of communication, the time, date and duration of a communication etc) derived from electronic communications will be covered. This data will have to be anonymized or deleted unless a user has given consent to their continued use or for legitimate purposes such as billing.

What about confidentiality ?

The proposed E-Privacy Regulation provides for a general confidentiality obligation for electronic communications data and does not allow for interference with that data (listening, scanning or through interception etc) unless

otherwise permitted under the proposed E-Privacy Regulation.

What about processing ?

The proposed E-Privacy Regulation sets out limited permitted purposes and conditions of processing communications data, e.g. if it is necessary to achieve the transmission of the communication and for the duration necessary for that purpose. Limitations are also set on processing electronic communications metadata, e.g. if it is necessary for billing, and, on electronic communications content, consent being paramount.

What about storage ?

The proposed E-Privacy Regulation also regulates storage, e.g. a provider of electronic communications service must erase electronic communications metadata or anonymise that data when it is no longer needed for the purpose of the transmission of a communication.

What about cookies ?

The rules about cookies (small pieces of data sent from a website and stored on a user's computer while the user is browsing) are being streamlined. No consent will be required for non-privacy intrusive cookies that improve internet experience, such as to remember shopping cart history, or, cookies set by a visited website that counts the number of visitors to that website.

What about spam ?

Unsolicited electronic communications by any means (emails, SMS, automated calls etc) are banned unless users have given their consent. This will also apply to marketing phone calls unless national law opts to allow consumers to object to the reception of voice-to-voice marketing calls such as by registering their number on a do-not call list.

What about sanctions ?

Fines for infringements of the proposed E-Privacy Regulation are aligned with GDPR - here the highest level of fine is 20 million Euros or 4% of total annual global turnover whichever is higher (see our GDPR FAQs [here](#) for more on this).

What about compensation ?

There is a right to compensation where an infringement of the proposed E-Privacy Regulation has caused material or non-material damage - the alleged infringer will have the burden of proof of demonstrating that they were not responsible for causing damage. Civil actions are likely.

Who will enforce the proposed new rules ?

The EU Member State data protection regulators will enforce the proposed E-Privacy Regulation.

When will the legislation be adopted ?

The aim is for the E-Privacy Regulation to apply from exactly the same time as the GDPR, i.e. from 25 May 2018. In terms of next steps the proposed E-Privacy Regulation will be considered by the European Parliament and the EU Council. Although the proposed E-Privacy Regulation is quite a short piece of legislation, whether it will get through the EU legislative pipeline in time for 25 May 2018 remains to be seen.

What about Brexit ?

In the context of Brexit, the UK's position as to whether the E-Privacy Regulation will become part of UK law or not once it has been fully adopted by the EU is unknown. However, simply in terms of timing, if the UK is still a member

of the EU when this legislation is adopted (May 2018) then this legislation will technically apply to the UK, even if only for a while until the Brexit process has been fully concluded. Because the UK government's officially declared position is to maintain the GDPR post-Brexit, it may well be that it also maintains the E-Privacy Regulation.

What should I be doing ?

Businesses should keep track on the progress of the proposed EU E-Privacy Regulation and start planning the changes that they are likely to need to make, such as regards cookies.

We write regularly and produce films about data protection and privacy issues which can be found [here](#). We have also developed a special fixed price solution to assist with compliance with EU GDPR called Cordery GDPR Navigator - more details about this can be found [here](#).

For more information please contact André Bywater or Jonathan Armstrong who are commercial lawyers with Cordery in London where their focus is on compliance issues.

[André Bywater](#), Cordery, Lexis House, 30 Farringdon Street, London, EC4A 4HH

Office: +44 (0)207 075 1785

andre.bywater@corderycompliance.com



[Jonathan Armstrong](#), Cordery, Lexis House, 30 Farringdon Street, London, EC4A 4HH

Office: +44 (0)207 075 1784

jonathan.armstrong@corderycompliance.com



