Confidentiality of electronic communications: Council agrees its position on ePrivacy rules

Today, member states agreed on a negotiating mandate for revised rules on the **protection of privacy and confidentiality in the use of electronic communications services**. These updated '**ePrivacy**' rules will define cases in which service providers are allowed to process electronic communications data or have access to data stored on end-users' devices. Today's agreement allows the **Portuguese presidency to start talks with the European Parliament** on the final text.

> Robust privacy rules are vital for creating and maintaining trust in a digital world. The path to the Council position has not been easy, but we now have a mandate that strikes a good balance between solid protection of the private life of individuals and fostering the development of new technologies and innovation. The Portuguese presidency is very pleased to launch talks now with the European Parliament on this key proposal.
>
> *Pedro Nuno Santos, Portuguese Minister for Infrastructure and Housing, President of the Council*

An update to the existing ePrivacy directive of 2002 is needed to cater for new technological and market developments, such as the current widespread use of Voice over IP, web-based email and messaging services, and the emergence of new techniques for tracking users' online behaviour.

The draft ePrivacy regulation will repeal the existing ePrivacy directive. As *lex specialis* to the general data protection regulation (GDPR), it will particularise and complement the GDPR. For example, in contrast to the GDPR, many ePrivacy provisions will apply to both natural and legal persons.

Council mandate

Under the Council mandate, the regulation will cover electronic communications **content** transmitted using publicly available services and networks, and **metadata** related to the communication. Metadata includes, for example, information on location and the time and recipient of communication. It is considered potentially as sensitive as the content.

To ensure full protection of privacy rights and to promote a trusted and secure **Internet of Things**, the rules will also cover machine-to-machine data transmitted via a public network.

The rules will apply when **end-users** are **in the EU**. This also covers cases where the processing takes place outside the EU or the service provider is established or located outside the EU.

As a main rule, **electronic communications data** will be **confidential**. Any interference, including listening to, monitoring and processing of data by anyone other than the end-user will be prohibited, except when permitted by the ePrivacy regulation.

Permitted processing of electronic communications data without the consent of the user includes, for example, ensuring the integrity of communications services, checking for the presence of malware or viruses, or cases where the service provider is bound by EU or member states' law for the prosecution of criminal offences or prevention of threats to public security.

Metadata may be processed for instance for billing, or for detecting or stopping fraudulent use. With the user's consent, service providers could, for example, use metadata to display traffic movements to help public authorities and transport operators to develop new infrastructure where it is most needed. Metadata may also be processed to protect users' vital interests, including for monitoring epidemics and their spread or in humanitarian emergencies, in particular natural and man-made disasters.

In certain cases, providers of electronic communications networks and services may process metadata for a purpose other than that for which it was collected, even when this is not based on the user's consent or certain provisions on legislative measures under EU or member state law. This processing for another purpose must be **compatible** with the initial purpose, and strong specific safeguards apply to it.

As the user's **terminal equipment**, including both hardware and software, may store highly personal information, such as photos and contact lists, the use of processing and storage capabilities and the collection of information from the device will only be allowed with the user's consent or for other specific transparent purposes laid down in the regulation.

The end-user should have a **genuine choice** on whether to accept **cookies** or similar identifiers. Making access to a website dependent on consent to the use of cookies for additional purposes as an alternative to a paywall will be allowed if the user is able to choose between that offer and an equivalent offer by the same provider that does not involve consenting to cookies.

To avoid **cookie consent fatigue**, an end-user will be able to give consent to the use of certain types of cookies by whitelisting one or several providers in their browser settings. Software providers will be encouraged to make it easy for users to set up and amend whitelists on their browsers and withdraw consent at any moment.

The text also includes rules on line identification, public directories, and unsolicited and direct marketing.

The regulation would enter into force 20 days after its publication in the EU

Official Journal, and would start to apply two years later.

Procedure

Today’s mandate was approved by ambassadors meeting in the Council’s Permanent Representatives Committee (Coreper).

The Commission presented its proposal in January 2017.

The Council and the European Parliament will negotiate the terms of the final text.