



Update on the **ePrivacy** Regulation

Privacy
March 2021

ECIJA

Analysis of the latest version of the Regulation on privacy and protection of personal data in electronic communications.

The latest version of the Regulation on privacy and the protection of personal data in electronic communications (the ePrivacy Regulation) was presented last February. As its predecessor, the ePrivacy Directive, this text will remain one of the fundamental pillars of the regulation on digital rights and the protection of users' information.

At the time of the elaboration of this note, the **Directive 2002/58 on Privacy and Electronic Communications** or **ePrivacy Directive** (which in Spain has been implemented through the **Information Society Services Law 34/2002, the LSSI**) is in force in Europe. The **ePrivacy Regulation** has gone through one of its last steps for its approval in February, with the publication of a new draft (which should be very close to the final one) to be debated by the European Parliament.

In this sense, this note is intended to detail the main new features and issues addressed by the ePrivacy Regulation. However, it should be noted that the contents thereof may undergo variations before its final publication and application.

By way of introduction, **the ePrivacy Regulation includes, within its scope of application, the processing of electronic communications, their contents and metadata referring to end users located in the European Union.** It also applies to the **protection of information on the terminals and devices of such users, to the offering of public directories of end users** or to the **sending of commercial communications by electronic means to such users.**

These activities must be carried out by a **provider of information society services** (hereinafter, the "Provider") **that is located in the European Union or that has access to the information indicated in the previous paragraph about citizens of the Union¹.** The following is a summary of what is new:

- 1 The Regulation lays down the cases in which the processing of data, content and metadata of electronic communications is authorised and in which cases it will be necessary to obtain the consent of the end user. 
- 2 Caller ID restriction, blocking of unwanted incoming calls, etc. 
- 3 There is provision for consent to be obtained through the browser, requesting the user to choose a specific configuration at the time of installation of cookies and other trackers, which can also be easily modified at any time. 
- 4 Commercial communications to customers: the opt-out system (right of objection) is maintained as long as the communication refers to the marketing of own contracted products or services. 
- 5 Penalties may amount to between EUR 10 million or 2% of the company's profits or EUR 20 million or 4% of the company's profits, similar to the GDPR limit. 

¹ The ePrivacy Regulation has not yet been translated into Spanish, thus the nomenclature of some terms may differ from the final Spanish version.



1. CONSENT

Regarding consent, the ePrivacy Regulation adopts as **valid the provisions contained in the General Data Protection Regulation (GDPR) for the granting of consent, both for individuals and legal entities**. This last point was not defined as such in the GDPR.

Also, one of the new features introduced is that **consent provided directly by a user prevails over that given using the settings of the computer programs, where possible**. This last point is fundamental, **since it is clear that consent can be obtained through the configuration, for example, of the browser**.

In turn, in those cases in which a provider cannot identify the data subject, **the technical protocol demonstrating that consent was given from equipment connected to the interface of a public telecommunications network for transmitting, processing or receiving information will be sufficient**.

Those users who consent to the processing of electronic communications data will have to be reminded periodically (at least every 12 months and as long as the processing persists) of the possibility of withdrawing the consent given. This obligation will disappear only if a user has requested not to receive such reminders.

In relation **to the processing of electronic communications data**, it will only be allowed when it is **necessary to provide the electronic communications service, to detect or prevent security risks or cyber-attacks or because it is necessary to comply with a legal obligation**.

Except for the last case, **the processing will only be allowed for the period necessary for the established purpose or, if this cannot be fulfilled, by anonymizing the data**.

With respect to the content of electronic communications, providers may only process, among others, text, voice, video, images and sounds, without prejudice to the aforementioned:

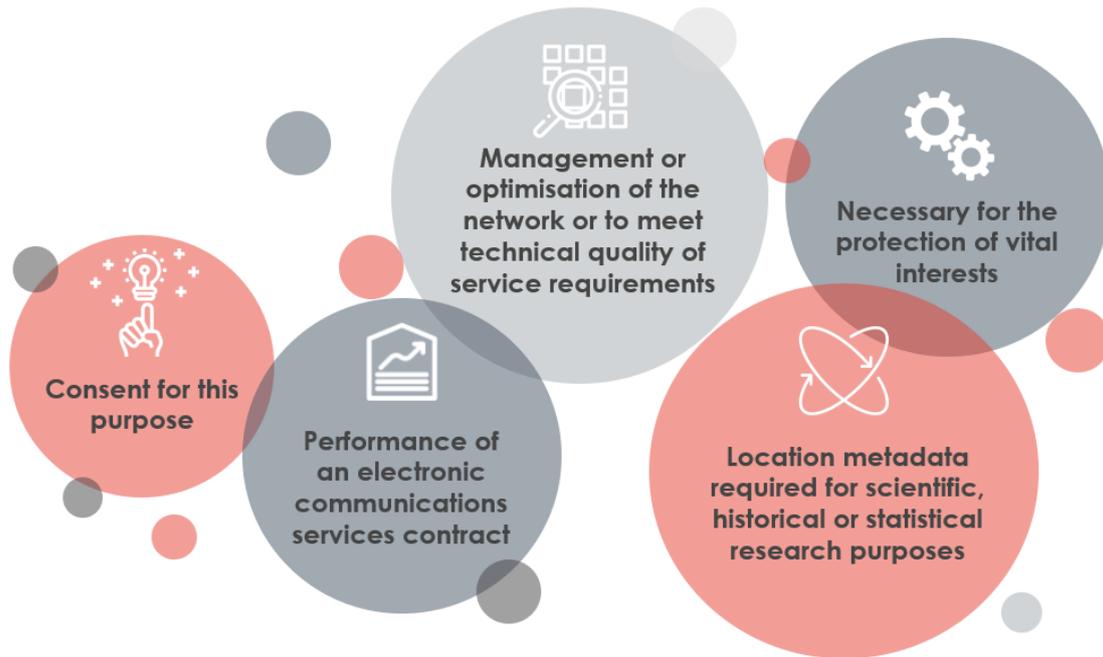
- When, **with the user's consent and for his individual use, it is required to provide a requested service**; or
- **If all end users concerned have given their consent to the processing of their content for one or more specific purposes**. In this case, **it will be necessary to carry out a Privacy Impact Assessment (PIA) beforehand to analyse the impact on the intended processing and, where required, consult the competent supervisory authority**.

In the same way as mentioned above, there are some scenarios in which the **processing of metadata in electronic communications** will be allowed **and, therefore, of data that will make it possible to trace and identify the origin and destination of a communication, the location of the device, as well as the date, time, duration and type of communication, and namely:**

- If it is **necessary for network management or optimization purposes** or to meet **technical service quality requirements**.
- For the **execution of a contract for electronic communications services**, or if necessary, **for billing, calculation of interconnection payments, detection or cessation of fraudulent or abusive use of electronic communications services or subscription to the same**.
- In case of having given a **consent** for such purpose.
- Because it is necessary for the **protection of vital interests**.



- Regarding the **location metadata necessary for scientific, historical or statistical research purposes**, complying with a series of requirements.
- With regard to the rest of the metadata also necessary for the purposes indicated in the previous point, **adequate guarantees will be required in accordance with the provisions of Article 21.6) and 89.1), 2) and 4) of the GDPR.**



With respect to **the processing of metadata considered compatible in electronic communications, when the processing is for a purpose other than that for which it was initially collected, and is not based on the consent of the user or on a rule of a Member State or of the Union**, the provider is required to **check whether the processing of the metadata for this new purpose is compatible with that initially provided for**, taking into account aspects such as the relationship between the initial and new purpose, the context in which the metadata were collected, the relationship between the user and the provider, the nature of the metadata, the consequences for the user of the new processing and whether there are adequate safeguards, such as encryption and pseudonymization of the data.

In case this processing is considered compatible, it can only be carried out considering that:

- **the processing cannot be carried out with anonymized information**, and that the metadata is deleted or anonymized as soon as it is no longer necessary for the intended purpose;
- **the processing is limited to pseudonymised metadata**; and
- **the metadata is not used to determine the nature, characteristics or to build a user profile.**

Finally, the ePrivacy Regulation obliges providers to **delete or anonymize data when it is no longer necessary for the intended purposes or, in certain cases**, when it is no longer necessary for the provision of an electronic communications service.



2. COOKIES AND SIMILAR TECHNOLOGIES

Other point introduced in the ePrivacy Regulation and worth noting is regarding the innovations related to cookies and similar technologies.

In this sense, the general rule is **the prohibition of the processing of such information, unless:**

- Such **processing is necessary to provide the electronic communications service.**
- **The user has consented to it.**
- **It is strictly necessary to provide a service specifically required by the end user.**
- **It is necessary for the purpose of audience measurement.**
- **It is necessary for security purposes, fraud prevention or detection of technical failures.**
- It is **required for a software update**, provided that it is necessary, the user is informed, and the end user can turn off the automatic installation of such updates.
- **It is necessary to locate the end user's terminal in an emergency call.**

In the event that the information collected is to be used for a different purpose, the provider shall analyse the compatibility of such purposes, taking into account the relationship between the initial and subsequent processing, the context and the relationship between the end user and the provider, the nature and modalities of the subsequent processing and the existence of additional measures, such as encryption and pseudonymization.

As analysed in the previous point, the processing **will only be lawful if the information is erased or anonymized when it is no longer necessary, the processing refers to pseudonymized information and the information is not used to determine the nature or characteristics of the end user or to build a profile of the end user.**

3. CONTROL OVER ELECTRONIC COMMUNICATIONS AND COMMERCIAL CALLS

Chapter III regulates the rights of end users in relation to the control over electronic communications. Articles 12 and 13 of the ePrivacy Regulation **establish rules applicable to the identification of subscribers.** For example, **the right to prevent, by means of a simple and free procedure, the presentation of the user's line identification in outgoing calls (contained in Art. 47.1 (m)) must now be exercisable on a per-call, per-connection or permanent basis.** In addition, **a new right has been introduced which focuses on the possibility of preventing the called user from presenting the identification of the line to which the caller is connected.** All these rights must include calls made to or originating in the Member States, and therefore have a European scope.

The **exceptions to the abovementioned rights apply, on the one hand, to cases of calls by emergency call services or those made to emergency services such as 112.** On the other hand, a **specific exception is added for cases where the end user has prevented access to the Global Navigation Satellite System (GNSS) of his terminal equipment: in the event of an emergency call, this service will be able to access the geolocation of the terminal equipment from which the user is calling for the "purpose of responding to this type of call".**

Regarding unsolicited calls, Article 14 of the ePrivacy Regulation leaves **it up to the Member States to develop specific guidelines to regulate the obligations of operators to temporarily identify callers in the event that the called user requests the monitoring of unsolicited or malicious calls.** The Regulation also recalls **that operators must offer**



subscribers, free of charge, the possibility of blocking incoming calls from specific, anonymous numbers or with a specific prefix or code, where technically possible, and of stopping automatic call forwarding by a third party to the user's terminal equipment.

As a general rule, **inclusion in public directories may only be made with the consent of the subscriber**. However, **Member States are given leeway for the inclusion of subscribers' numbers in directories without their consent, provided that the subscriber can object to such inclusion**. Art. 15.4a clarifies that, **for all numbers included in directories prior to the entry into force of the ePrivacy Regulation, such numbers may be retained unless the subscriber has expressed his objection**.

Finally, art. 16 establishes **rules concerning the sending of unsolicited commercial communications**. As a general rule, **mailings may only be sent with the consent of the recipient**. However, as an exception, **legitimate interest is still considered as valid, provided that the recipient has been given the opportunity to object to the sending of commercial communications both at the time of collection of his or her data for this purpose and in each of the communications**.

Additionally, **each communication will have to identify the sender and use an effective return address, which could mean that it would no longer be valid to send commercial communications only indicating a "noreply" addresses**. Finally, the ePrivacy Regulation clarifies that **Member States will be able to establish the periods of time from the purchase of a product or service during which a user would be considered a customer**.

With respect to penalties, it is determined that each end user will have the right to make a complaint about breaches of the ePrivacy Regulation and **may receive financial compensation for such breaches**.

Penalties may be graduated between ten million euros or 2% of the company's profits or twenty million euros or 4% of the company's profits, similar to the framework imposed by the GDPR.

Finally, **the ePrivacy Regulation, when finally published, will have 24 months to be fully implemented, repealing the previous ePrivacy Directive**.

Data Protection and Privacy Area

+ 34 91 781 61 60
info@ecija.com



ECIJA

Torre de Cristal
Pº de la Castellana, 259C
28046 Madrid

www.ecija.com