



AEPD Guide on the use of cookies and similar technologies

November 2019

On Friday 8 November, the Spanish Data Protection Agency (the “**AEPD**”) published its guide on the use of cookies and similar technologies (the “**Guide**”). The Guide updates the criteria established six years ago by the AEPD on the use of these technologies that became outdated with the implementation of European Data Protection Regulation 2016/679 (the “**GDPR**”) and Basic Law 3/2018 on the Protection of Personal Data and Guarantee of Digital Rights. This newsletter highlights the points that we consider most important about the Guide and which should therefore be taken into account when reviewing and updating cookies policies.

What does the Guide address?

The Guide provides guidance on how to comply with the obligations set out in the special rule regulating the use of cookies and similar technologies, such as web beacons or bugs, which is art. 22 of Law 34/2002 on Information Society Services and Electronic Commerce, in light of the new legal framework for data protection. The Guide points out that these obligations are also applicable to fingerprinting techniques. Those obligations are, specifically, the fulfilment of the duty of transparency and the collection of users’ informed consent.

To whom does the Guide apply?

Information society service providers who install, on websites or in mobile applications, cookies or similar technologies the use of which requires users’ informed consent. Within the category of cookies that require consent are those that are not strictly necessary for the purposes of allowing communication between the user and the network or providing a service required by the user. For instance, first-party or third-party analytical or statistical cookies and behavioural advertising cookies are subject to consent. With respect to cookies exempt from this obligation (e.g. technical cookies), the AEPD recommends reporting on their use.

How should the transparency principle be complied with?

The AEPD, as it recommended in its previous guide, proposes that information should be provided through a layer system, although other ways of displaying the information could be considered (e.g. offline media or by informing when registration for a service is requested). The first layer (the cookie banner) should include the essential information about the use of cookies and the second layer (i.e. the complete cookies policy) should provide the rest of the required information. This information should be distributed as follows:

FIRST INFORMATION LAYER	SECOND INFORMATION LAYER
a) Identification of the publisher in charge of the website.	a) Definition and generic function of cookies.
b) Identification of the purposes of the cookies to be used.	b) Information about the type of cookies used and their purpose.
c) Identification of whether the cookies are first-party or third-party cookies.	c) Identification of who uses the cookies.
d) Generic information about the type of data to be collected and used, in the event that user profiles are developed.	d) Information about how to accept, reject or revoke consent or delete cookies.
e) Information about how to accept, configure, and reject cookies, specifying which actions will imply the user's acceptance of the use of cookies.	e) Information on international transfers to third-party countries carried out by the publisher of the website or mobile application.
f) Clearly visible link to a second information layer that includes more detailed information about cookies (i.e. the cookie policy).	f) Information about the logic used, as well as the relevance and expected consequences, when developing profiles involving automated decision-making with legal effects for users or significantly affecting them in a similar way.
g) Direct link to the cookie configuration panel.	g) Information about the period of time personal data will be stored.
	h) The rest of the information required by Art. 13 of the GDPR (e.g. the rights of data subjects) may be facilitated by referring users to the privacy policy.

Furthermore, the AEPD points out that:

- information should be brief and succinct “to avoid information overload”; and
- the use of confusing sentences such as “*we use cookies to personalise your content and create a better experience for you*” or “*to improve your navigation*”, or wording such as “*we may use your personal data to provide personalised services*”, to refer to advertising cookies that store information about user behaviour through the analysis of browsing habits (i.e. profiling), should be avoided.

How should the obligation to obtain informed consent be fulfilled?

The main novelty of the Guide is that, unlike those published by other European authorities, the option to “*continue browsing*” is accepted as a valid formula to obtain users’ unambiguous consent in some cases. The AEPD points out that this option may be more appropriate for registered users and warns that it may lead to greater difficulties in proving the collection of consent and that the validity of this system will depend, to a large extent, on the quality and accessibility of the information provided and the type of action from which consent is inferred (e.g. navigating to a different section of the website, closing the first-layer notice or clicking on some piece of the service’s content). Likewise, procedures must be incorporated so that refusing consent is as simple as giving it. For this reason, a button to reject all cookies must be enabled in the cookie configuration panel.

However, the formula for obtaining unambiguous consent (of the “*continue browsing*” type) will not be valid in those cases in which cookies are used to carry out processing that requires explicit consent. In particular, an “*I accept*” button should be included in the cookie banner in cases in which special categories of personal data are processed, automated individual decisions are made with legal effects on users (the legal basis of which is consent), or international data transfers are carried out and the legal basis for doing so is consent.

Other issues to consider

The Guide points out other issues that could be relevant, including the following:

- *Cookie configuration panel.* The information about the first-layer cookies must be completed with a system or configuration panel in which the user can choose whether or not to accept cookies in a granular form, or a link that leads to that system or panel. The link or button to manage cookie preferences must take the user directly to the configuration panel, which may be integrated into the second information layer. The Guide states that, in order to facilitate the selection of cookies by the user, two buttons may be implemented in that panel: one to accept all cookies and another to reject all cookies, with this option being more strongly recommended the greater the number of different cookies used. If the “*continue browsing*” method is used as a means of obtaining consent, a button for rejecting all cookies must be included in the panel, as indicated above, in order to respect the requirement that it should be as easy to withdraw consent as it is to give it.
- *Temporary duration of cookies.* The AEPD recommends the preferential use of session cookies, instead of persistent cookies. If it is necessary to use persistent cookies, the AEPD indicates that their duration should be kept to the minimum necessary to achieve the purpose of their use.
- *Consent update.* The Guide highlights, as good practice, that the validity of consent for the use of a given cookie should not exceed two years.
- *Websites aimed at children under 14.* Mechanisms should be implemented to verify that consent to the processing of personal data is given by the person holding parental authority and comply with the principle of data minimisation.
- *Possibility of denying access to the service in the case of the rejection of cookies.* The AEPD recognises the possibility of denying access to an information society service if cookies are not accepted. However, such access may not be restricted in cases in which the refusal prevents the user from exercising a legally recognised right, for example if access to that website is the only means provided to the user to exercise that right.
- *Possible impact of the (EU) Regulation on privacy and electronic communications.* It should be kept in mind that the Guide could be amended when this Regulation is published; it is currently still at the proposal stage.

We remain at your disposal to analyse in greater depth any questions relating to the use of cookies and similar technologies that you may have on your websites.

Contact lawyers



Leticia López-Lapuente

Partner

+34 915860727

leticia.lopez-lapuente@uria.com



Reyes Bermejo

Managing associate

+34 963531766

reyes.bermejo@uria.com



Laia Reyes

Senior associate

+34 915870903

laia.reyes@uria.com

BARCELONA
BILBAO
LISBOA
MADRID
PORTO
VALENCIA
BRUXELLES
LONDON
NEW YORK
BOGOTÁ
CIUDAD DE MÉXICO
LIMA
SANTIAGO DE CHILE
BEIJING

www.uria.com

This newsletter provides general information and does not constitute legal advice