ECIJA | Torre de Cristal Pº de la Castellana, 259C
28046 Madrid · Tel: +34 917 816 160
www.ecija.com

AEPD Guide on the use of cookies

Madrid, November 12th 2019

Last Friday, 8 November 2019, the Spanish Data Protection Agency ("AEPD") published the new *Guide on the use of cookies*, with the aim of updating its criteria for the appropriate use of cookies to the requirements of the GDPR and the current cookie technology and cookie-management tools.

This Article has been drafted with the purpose of summarising the obligations derived from the *Guide on the use of cookies* and must be construed in addition to the recent judicial and administrative case-law laying down tips and criteria for an appropriate use of cookies which we have already analysed in our Informative Note of 14 October 2019.

(I) Cookies exempted from the requirement of informed consent

First, the AEPD lays down the exact scope of Article 22.2 of the Spanish Information Society Services Act ("**ISSA**"), derived from Article 5.3 of Directive 2002/58/EC, whereby cookies can only be used with the informed consent of the user. The AEPD adheres to the Article 29 Working Party's Opinion 04/2012 on Cookie Consent Exemption to determine that a **cookie (i) used for the sole purpose of carrying out the transmission of a communication over an electronic communications network** or **(ii) strictly necessary to provide a service which has been explicitly requested by the user** will not fall within the scope of application of Article 22.2 and hence **may be used without informing the user or obtaining his or her consent.**

(II) Information to be provided

Article 22.2 ISSA specifies that, prior to requesting his or her consent, the user must obtain clear and complete information about the use of cookies and, where appropriate, about the processing of his or her personal data in accordance with the regulations on personal data protection. This indicates that the user should be able to understand the mechanism and purposes of the cookies used though a website.

As information must be given in a first stage for the consent to be valid, the AEPD recommends to display it in two layers, so that the essential details on the use of cookies will automatically appear within a banner or within a consent management platform ("**CMP**") as soon as the user enters the website, while further information can be found in a second layer ("**cookie policy**") to which the user can access voluntarily.

The first layer shall include the following details:

(i) **Identity of the publishe**r of the website (just a name or trademark; a registered company name shall not be necessary as this information will be available in the second layer);
(ii) The **purposes for which the cookies will be used**;
(iii) Indication as to **whether the cookies will be used only by the publisher** (first-party cookies) **or also by third parties** (third-party cookies)
(iv) Generic information on the type of data used for advertising purposes, where appropriate;

(v) **The way the user will be able to consent or reject the use of cookies** (the conditions for obtaining consent are explained below);

(vi) A **clearly visible link to the cookie policy**.

As for the second layer or cookie policy, it must be easily and permanently accessible from any section of the website and gather the information necessary for the average user of the website to understand how cookies work and for what purposes they will be installed, together with all the information required by Article 13 of Regulation (EU) 2016/679 (General Data Protection Regulation or "**GDPR**") in the event that personal data are being collected.

(III) Conditions for consent

The AEPD reminds that under Article 4 GDPR a valid consent to one specific purpose must be given by means of a clear affirmative action performed by the user in full awareness of the consequences of such action. Moreover, **it must be as easy to withdraw as to give consent. Additionally,** no cookie may be installed on user's device before his or her prior validly given consent.

In consideration thereof, **the user must be given the chance to accept or reject all cookies or to select the specific purposes for which cookies may be installed**.

Also, the user may be informed that **he or she can accept the cookies by just continuing to browse the website**, as long as he or she can withdraw consent as easily as he or she consented through granular consent approach. In no case access to the second layer may be deemed as an acceptance to the use of cookies.

(IV) Consent management platforms

The Guide **highly recommends the use of CMP's** to demonstrate compliance with the duty to obtain a valid informed consent from the user.

A CMP allows the user to select the purposes for which cookies may be installed, as well as to access through links to further information directly provided by the managers of the different cookies.

(V) Conditions applicable to child's consent

For websites where the average users are under-fourteens, a publisher shall be required to **apply an additional effort to verify that consent of the user is given by his or her parents or legal guardians**. Further, it shall be kept in mind the need to strengthen the data protection guarantees of the users, specially in relation to the data minimisation principle.

For example, the AEPD states that if a website obtains data solely for analytical purposes, a valid consent may be obtained by installing a prior warning which informs the user of the need to ask his or her parents or guardians to give consent on his or her behalf.

(VI) Possibility to deny access if consent is not given

Access to a website may be denied to a user who does not consent to the use of cookies (including advertising cookies) provided that denial does not prevent the exercise of a right.

(VII) Responsibility

The AEPD considers that Article 22.2 of ISSA does not define who shall be responsible for informing and obtaining consent. **Thus, it esteems that both the publisher and those third parties managing cookies as data controllers shall coordinate to comply with these tasks.**

Notwithstanding the above, if a publisher uses a CMP which allows said third parties to directly inform the users and record consents, then the third parties will be individually responsible for informing and obtaining consent.

The AEPD reminds that some entities which create and manage their own cookies, such as media agencies or trading desks, will usually use their cookies on behalf of several advertisers as data processors; thus, a misuse of cookies by that processor will lead to independent liabilities of these advertisers. **There is no way to transfer that responsibility from the controller to the processor before a supervisory authority**, though a comprehensive set of contractual guarantees and obligations may require the processor to compensate the controller for any sanctions, damages or injunctive relief arising from a wrongful use of the processor's cookies.

ECIJA's Privacy and Data Protection Area
info@ecija.com
Phone: + 34 91.781.61.60

ANNEX

Issue	France	Germany	Spain	U.K.
Grace period	Six months after the publication of a (yet to be issued) opinion from the CNIL discussing how to obtain consent in practice	X	X	X
Same requirements to similar technologies (pixels, tags, beacons)	✓	✓	✓	✓
Browsing consent	X	X	✓ The user consent could be collected just with user browser navigation if (i) clear information is provided; (ii) a cookie configurator is implemented; (iii) a clear rejection button is implemented	X
Are cookie walls allowed?	X	X	X Denial of access shall not constrict individual user rights (for example, if the website is the only mean to exercise such rights)	X If GDPR requirements are evaluated against other rights, the denial of access could be implemented
Do analytic cookies require consent?	Not in all the scenarios. CNIL Deliberation 2019-093 article 5 defines consent exception requirements for analytic purposes	Not in all the scenarios. Consent required if analytic cookies lead to a transfer of personal data to a third party	✓ The only exception are the cookies "strictly necessary" defined by Recommendation 4/2012 WP29	✓ The only exception are the cookies "strictly necessary" defined by Recommendation 4/2012 WP29
Other lawful bases possible?	The Deliberation is focused in consent, but other bases are not clearly defined	Contract performance and legitimate interests (even for analytics purposes) are possible legal bases.	Consent is mandatory for all the cookies not excepted by Recommendation 4/2012 WP29	Generally, legitimate interest is not the appropriate lawful basis for the processing of personal data relating to cookies. Legitimate interest will never be the lawful basis for profiling processing of personal data

Special requirements regarding options given to users	X	X Just an OK button is not enough, granular options (for each data processing activity) shall be provided to the user	X Only if continue browsing consent is implemented, a clear option to reject all shall be implemented	✓ Agree/allow buttons shall be emphasized over Reject/block options
Cookie configurator	Not mandatory, but user shall be able to express his/her granulated consent	Not mandatory, but user shall be able to express his/her granulated consent	✓ Mandatory	Not mandatory, but user shall be able to express his/her granulated consent
Cookie lifespan and retention periods	Consent-excepted analytic cookies lifespan must not exceed 13 months. Information collected through the trackers can be kept for a maximum of 25 months	X	X The guide just refers to article 13 GDPR. Notwithstanding, the conservation of the user consent must be kept for a maximum of 24 months	X
Data processed	Even if cookie does not process personal data, Directive 2002/58/CE article 5 (39) applies	Not defined.	Even if cookie does not process personal data, Directive 2002/58/CE article 5 (39) applies	Even if cookie does not process personal data, Directive 2002/58/CE article 5 (39) applies
Roles of the parties	Could be joint controllers, processors or independent controllers (depending means and purposes)	Not defined	Controller defines the means and purposes (even if it is processed through a processor). Joint controller should also be considered	The person setting the cookie is primarily responsible for compliance, although this is not necessarily the case where multiple parties are involved

ECIJA's Privacy and Data Protection Area
info@ecija.com
Phone: + 34 91.781.61.60