LK SHIELDS
YOUR LEGAL COUNSEL

TECHNOLOGY

The Data Protection Commission is Undertaking a Cookies Sweep

by **lk-shields**

The Data Protection Commission is Undertaking a Cookies Sweep

4th October 2019 | by

The Special Investigations Unit of the Data Protection Commission (DPC) has been contacting website operators in Ireland requesting their participation in a cookies sweep survey.

We understand that the purpose of this sweep is to obtain information which will enable the DPC to review the current levels of compliance with Irish privacy and data protection laws when deploying cookies and similar technologies on or through websites and apps. This involves asking selected website operators to provide detailed information on how they use cookies, how this is explained to subscribers and users, and how their valid consent is obtained.

We understand that these sweep surveys are grounded on Article 31 of the GDPR, which requires controllers and processors to cooperate with the DPC, if requested, in respect of the performance of its statutory tasks. Participation is not optional. A refusal to participate could result in enforcement measures.

General rules on the use of cookies and similar technologies

The European Communities (Electronic Communications Networks and Services) (Privacy and Electronic Communications) Regulations 2011 (ePrivacy Regulations) gives effect in Ireland to EU Directive 2002/58/EC (as amended).

The ePrivacy Regulations apply to certain types of processing, including the use of cookies and similar technologies (e.g. SDK, pixels, tags, browser fingerprinting), and must be read together with the GDPR and the Data Protection Act 2018 if the use of those technologies involve the processing of personal data.

Generally, user consent is required before setting non-essential cookies and similar technologies used to store or gain access to information on a user's device. Users must be provided with easily accessible, 'clear and comprehensive' information on the technology being used and its purpose.

The CJEU's recent ruling (Case C?673/17) in Planet49 provides that the standard of consent that must be obtained from users in order to comply with the ePrivacy Regulations, is based on the definition of, and the conditions for, valid consent under Articles 4(11) and 7 of the GDPR (i.e. a clear, affirmative act, freely given, specific, informed, and unambiguous), even if the activity does not involve the processing personal data.

Recital 32 of the GDPR prohibits pre-ticked boxes, and provides that silence or inactivity does not constitute valid consent. The CJEU's ruling in Planet49 confirms this in respect of obtaining valid consent for cookies - an active action by the user is required to signify their consent.

Consent is not required if the cookie or other technology is:

- used for the sole purpose of carrying out the transmission of a communication; or
- 'strictly necessary' in order to provide an online service explicitly required by the user (e.g. essential cookies used to remember the contents of a user's online shopping basket; or to comply with security obligations mandated by law).

To provide 'clear and comprehensive' information on the use of cookies, and to obtain valid consent, a website should provide a user friendly consent (opt-in) mechanism, supported by a cookies notice, an Article 13 GDPR compliant privacy notice (where the use of cookies involves processing personal data) and other consent management tools.

Proposal for an EU-wide ePrivacy Regulation to replace Directive 2002/58/EC

A proposed EU-wide ePrivacy Regulation, intended to replace Directive 2002/58/EC, is anticipated to introduce simplified rules on cookies including by extending the current consent exemptions. Whilst the European Parliament adopted the proposed Regulation in October 2017, it remains in draft. The most recent version was issued on 18 September 2019, but the timing for the formal adoption of the Regulation remains uncertain. The DPC's current cookies sweep is not based on this draft EU Regulation.

Demonstrating compliance

We understand that participants in the sweep have been requested to demonstrate the steps they have taken to comply with Regulation 5 of the ePrivacy Regulations, as it applies to their use of cookies and similar technologies, and specifically to demonstrate how the consents obtained comply with the GDPR's standard for valid consent.

In order to assist the DPC in assessing current levels of compliance, we understand that participants have been requested to provide detailed information and materials relating to their use of cookies and similar technologies, including:

- Details of all cookies and similar technologies currently used, including their names, functions, security, origin and duration, whether first-party or third-party, whether essential or optional and the methodology used to determine whether a cookie is essential or optional.
- Information demonstrating how users' consent is obtained before the deployment of cookies and similar technologies, and how this consent meets the GDPR's requirements for valid consent.
- Copies of website privacy notices and cookies notices, information on how these are presented to users and all information available on the website or app relating to the use of cookies and similar technologies, including screenshots of any cookies banners, preference centres, etc.
- The reason(s) for any non-compliance with the ePrivacy Regulations on the part of the participant, the steps taken and the expected time line for rectification of any non-compliance.

Why is the DPC carrying out this cookies sweep?

Cookies sweeps are not a new initiative. The European Data Protection Board (EDPB), under its previous guise of the Article 29 Working Party, coordinated a cookies sweep of 478 websites across eight EU member states in 2014. This sweep was carried out before the higher standards for consent were introduced by the GDPR. Ireland did not take part in that sweep.

The DPC's cookies sweep is not unexpected. Whilst there is no mention of the sweep on its website, DPC representatives have previously indicated that cookie-based transparency and consent is on the DPC's agenda for the second half of 2019.

Cookies consent is topical across Europe. For example, on 1 October 2019, the CJEU provided its judgment in the Planet49 case concerning cookie-based transparency and consent. Whilst the CJEU's judgment deals with consent under the ePrivacy Directive, its judgment indicates that inferred consent from passive activities (e.g. continued browsing of a website) may not be valid. This view is supported by recent guidance issued by data protection authorities in France, Germany and the UK.

What should organisations be doing now?

Below are some key initial steps when reviewing your organisation's level of compliance with current laws relating to the use of cookies and similar technologies.

- **Audit:** Conduct a review, and prepare an inventory, of all cookies and similar technologies currently used by your websites and apps. Establish whether appropriate arrangements are in place for the use of any third-party cookies, including what information is shared with any third party, how it is shared, and how users are informed of this. If you identify any cookies that are no longer needed, you should consider removing them.
- **Cookies Notice:** Following your audit, consider refreshing your cookies notice. 'Clear and comprehensive information' 'in accordance with data protection law' must be given to users in respect of the use of cookies and similar technologies, including those from other services such as online advertising networks or social media platforms. In order to satisfy the consent requirements under the ePrivacy Directive, the CJEU's Planet49 ruling requires controllers to disclose the duration of cookie retention and the sharing of cookies with third parties.
- **Privacy Notice:** To the extent your use of cookies and similar technologies involves the processing of personal data, this activity should be identified in a privacy notice. This will involve specifying the legal grounds upon which you rely for processing this personal data. Whilst the ePrivacy Regulations require that users must provide consent before non-essential cookies are dropped on their terminal equipment, a controller may be able to rely on an alternative legal grounds for subsequent processing beyond the setting of any cookies. This approach should be carefully considered, particularly if the subsequent processing may involve third party sharing.
- **Consent:** Consider how users currently provide their consent to non-essential cookies, and whether the consent obtained meets the GDPR's requirements. Users must take a clear and positive action to give their consent to non-essential cookies, and so pre-ticked boxes (or equivalents) are not appropriate. Further, inferring consent from continued browsing may not amount to valid consent for the use of cookies, and this is indeed the view of a number of EU data protection authorities.

About the Author