LK SHIELDS
YOUR LEGAL COUNSEL

INTELLECTUAL PROPERTY

Cookie Fumbles: Grace Period in Ireland Ends Soon

by **lk-shields**

Cookie Fumbles: Grace Period in Ireland Ends Soon

5th August 2020 | by

The DPC's six-month grace period to bring websites and apps into compliance with Irish cookies rules expires on 5 October 2020.

After this date, the DPC will consider taking enforcement action against non-compliant operators. In this note, we take a look at some of the key requirements under the DPC's cookies guidance and why controllers located in other EU member states and beyond should be aware of these.

Cookies Sweep

During the second half of 2019, the Data Protection Commission (DPC) undertook an examination of cross-sector levels of compliance with Irish privacy and data protection laws when deploying cookies and other tracking technologies through websites and apps. As outlined in our previous publication, the main purpose of the sweep was to assess whether GDPR standard consent is being obtained for the use of cookies and other tracking technologies, and to use these findings to develop its updated cookies guidance.

The DPC's cookies sweep report, published 6 April 2020, identified a significant lack of compliance with ePrivacy laws by a number of websites and apps operating on the Irish market. Overall, the DPC's sweep of 38 websites and apps revealed widespread deficiencies and stated that this *"suggests a more systemic issue that must be tackled firstly with the publication of new guidance, followed by possible enforcement action where controllers fail to voluntarily bring themselves into compliance*."

The DPC published its guidance on 6 April 2020 and provided a six-month grace period from that date before it considers taking enforcement measures.

Cookies In Practice

Below are some of the key considerations for an operator planning to deploy cookies and other tracking technologies in Ireland.

Consent

User consent must be obtained before any non-necessary cookies or other tracking technologies are stored on or accessed from a user's device. This consent must meet the high standards for consent under the GDPR (i.e. a clear affirmative act, freely given, specific, informed and unambiguous) and this applies even if a cookie does not involve the processing of personal data.

Operators can no longer imply a user's consent. For example, cookie banners that tell users that by continuing to browse the website they consent to cookies, or banners that disappear when a user scrolls or clicks any part of a webpage, or cookie settings that are pre-selected to 'ON' (or similar) are unlawful. Also, users' browser settings cannot be relied upon to infer consent.

It is not necessary to obtain consent individually for each cookie. Instead, it should be obtained for each purpose for which cookies are used. In practice, operators may classify cookies according to their type and purpose and seek user consent for each category, rather than for each cookie separately.

‘Strictly Necessary’ Cookies

Cookies which are “*strictly necessary in order to provide an information society service explicitly requested by the subscriber or user*” do not require consent. However, this is a narrow exemption that must be carefully applied. The DPC reported that a number of participants in its cookie sweep had mis-identified cookies as being ‘strictly necessary’.

According to the DPC, analytics cookies do not benefit from this exemption. Therefore, first-party and third-party analytics cookies require GDPR standard consent before setting these on a user’s device. While the DPC stated that first-party analytics cookies are unlikely to be a priority for enforcement, third-party analytics are identified as a greater privacy risk and, as such, the validity of consent obtained for these appear to be one that the DPC will closely watch.

Cookies Inventory

In order to determine which cookies require consent, it is necessary to know exactly what cookies and tracking technologies are used and why they are used.

A common mistake by Irish operators has been to treat their cookies policy as a static document. However, as content and features are added to a website, such as embedded videos and maps, third party cookies that require consent are often set. Operators must be alive to this and maintain effective controls that monitor their platform for new cookies, update their consent framework to reflect these and cull cookies that are no longer needed.

Monitoring tools should be carefully selected. Using trial versions of cookie scanning software may only provide a partial scan of a website, meaning an inventory may be incomplete. The DPC’s cookies sweep report shows that it will carry out its own scan of websites and apps to identify whether an operator’s cookies consent framework identifies its entire inventory.

An operator should know, in respect of its inventory, the purposes of the various cookies and its relationship with third party providers. The duration of any cookie must be proportionate to its purpose or function, even if a cookie is ‘strictly necessary’. Operators should consider any default lifespans for persistent cookies they use. While a default lifespan may be appropriate for a particular purpose, this should be checked and changed if appropriate. Also, the DPC considers six months to be the appropriate time limit for consent to be retained after which time the user must be prompted to give their consent again.

Cookie Banners or Pop-Ups

Consent must be separate from other matters and cannot be bundled into terms and conditions or privacy notices. The DPC considers layered consent to be good practice. This is a common approach whereby a concise cookie banner or pop-up is displayed when a user lands on a website and which provides the first layer of information about the use of cookies. This should also include, as a second layer, a link or means of accessing further and more granular information (e.g. links to a cookies policy, privacy notice and cookies management functionality).

Cookie banners and pop-ups can include features to allow users to accept, reject or manage cookies. However, a banner that only gives the user the option to click 'accept' to say yes to cookies and which provides no other option is non-compliant. The DPC's guidance does not require banners and pop-ups to include a 'Reject All Cookies' option. However, a user must be given an option to see more information on the use of cookies (e.g. a 'Manage Cookies' option) and must not be "nudged" into accepting cookies over less privacy intrusive options. Therefore, equal prominence should be given to whatever options are provided on the banner. Also, the banner or pop-up must not obscure the text of any privacy notice or cookie policy.

Transparency

Users must be given clear and comprehensive information in accordance with Irish data protection law about the use of cookies. This requirement applies even if a cookie does not involve the processing of personal data. To the extent the use of cookies involves the processing of personal data, the controller must comply with the transparency requirements under Articles 12 to 14 of the GDPR.

The DPC's guidance highlights that accessibility for those with vision or reading impairments should be considered when designing user interfaces. For example, colour-coded sliders that are intended to signify consent may not be visible to all users.

Third Party Cookies

Where a platform sets third-party cookies, both the operator and the third party have a responsibility for ensuring users are clearly informed about cookies and for obtaining consent. The DPC's guidance reminds operators that using third party 'like' buttons, plugins or widgets, pixel trackers or social media-sharing tools may result in the website operator and the owner of these third-party assets being '*joint controllers*' for the purpose of Article 26 of the GDPR. Operators must assess the possible joint controller issues arising from the use of third-party assets and plugins, and ensure this is reflected in their cookies consent framework.

Consent Management Platforms (CMPs)

Users must be able to withdraw or vary their consent as easily as they gave it. In practice, the DPC supports the use of website controls (e.g. radio buttons or sliders) that allow users to choose what cookies are set and to change these choices at any time through the same functionality.

CMPs can be developed in-house or sourced externally to assist managing users' cookie choices and to help meet their transparency obligations. These systems typically consist of a template cookies banner that links to a preference centre through which users can see the cookies inventory and provide or withdraw consent as desired. Some of the more sophisticated third-party CMPs can provide regular scans for cookie inventory and settings to deal with consent requirements for specific jurisdictions.

It is imperative when using third-party CMP's to ensure that the settings reflect local ePrivacy law and guidance. The DPC's cookies sweep identified a number of examples of where CMPs had been deployed incorrectly and highlighted that this will be a "*priority for enforcement*".

In addition to ensuring the correct local settings for a CMP, it is important to ensure that the information and terminology provided in any cookies banner and preference centre are consistent with the cookies policy, privacy notice and any other user-facing information relating to same. Any disconnect between these could dilute the validity of consent.

Beyond Ireland

ePrivacy laws are not the same across the EU. The European Commission proposed a new EU Regulation to harmonise EU ePrivacy laws. This was intended to come into force at the same time as the GDPR, on 25 May 2018. However, there is no sign of finalised text so we will be operating under the current fragmented framework for the foreseeable future.

What this means in practice is that any operator, whether or not established in the EU, should consider the ePrivacy laws and cookies guidance in all of the EU member states it intends to deploy cookies and tracking technologies. Also, as privacy laws continue to evolve across the globe, operators should identify the rules in other geographic locations they intend to operate.

If placing and retrieving information through a cookie or other tracking technology involves the processing of personal data, this may trigger the material scope of both the ePrivacy Directive and the GDPR. Unlike the GDPR, the ePrivacy Directive does not include provisions dealing with its territorial scope. However, the effect of Article 3(2) of the GDPR is that a non-EEA platform that offers goods or services to data subjects in the EEA, or monitors their behaviour, will need to comply with the GDPR and the consent requirements under Article 5(3) of the ePrivacy Directive if its use of cookies involves the processing of their personal data.

The lack of harmonization on EU cookies rules is unfortunate. However, this will not deter national supervisory authorities scrutinising practices and possibly taking enforcement measures. This is a challenging prospect for most operators, but particularly the case for smaller enterprises that do not have the resources to ensure compliance in every geographic market they operate.

CMPs can be a cost-effective compliance aide, but their use should be carefully managed as part of an overall compliance framework. Also, as the DPC put it, *“privacy and cookie policies should be accurate and kept up to date. Using a template service to generate a privacy policy or cookie policy is a futile and cosmetic exercise. Similarly, controllers who have multiple websites must ensure that each of them has their own privacy policy which reflects the underlying reality of the processing”.*

About the Author