The DPC's new guidance on cookies

Mark Ellis, Senior Associate with McCann FitzGerald, discusses what can be learned from the DPC's position on the use of cookies, as set out in its recently published guidance

We have all grown accustomed to browsing the internet and being subjected to cookie banners and pop-ups arising on almost every new website we visit, as well as appearing on those websites to which we return time and again.

If it sometimes feels like 'cookie fatigue' has long since set in from a user perspective, it appears that, conversely, 2020 is a year in which the Data Protection Commission has chosen to focus on organisations' use of cookies. This is most evident from its April publication of the results from a survey (or 'sweep') it conducted on the use of cookies by a selection of 40 Irish websites across a wide range of sectors.

Following that cookies sweep and, informed by its findings, the DPC has also now published new guidance ('the Guidance', copy at www.pdp.ie/docs/10962) in order to clarify some misconceptions and to give revised general guidance on the use of cookies in Ireland.

As such, it is a good time to be clear on the scope of this renewed regulatory focus, and the DPC's position on the use of cookies and for organisations to improve their compliance in this area.

What are cookies and how are they regulated?

According to the Guidance, cookies are 'usually small text files stored on a device, such as a PC, a mobile device or any other device that can store information'. Most commonly, users are most aware of browser based cookies. However, as the DPC is keen to point out, other types of cookies and tracking cookies also come within the legal regime applying to cookies, including pixel trackers (or pixel gifs), 'like' buttons and social sharing tools, and device fingerprinting technologies. This is important to recognise as organisations continue to broaden their use of mobile apps and tracking abilities in marketing communications.

Regulation 5(3) of the European Communities (Electronic Communications Networks and Services) (Privacy and Electronic Communications) Regulations 2011 (the 'ePrivacy Regulations'), together with the GDPR, sets out the cookies (and similar technologies) consent legal requirements.

Organisations using cookies are required to provide 'clear and comprehensive information' to end users on their use of cookies, as well as seek consent for all types of cookies, unless an exception applies. Regulation 5(3) of the ePrivacy Regulations also requires that this clear and comprehensive information must be provided in a way which is 'prominently displayed and easily accessible', and must include information on the purposes of the cookies set.

There is an exception from the consent requirement for any cookies which are set on the user's equipment for the 'sole purpose of carrying out the transmission' or which are 'strictly necessary in order to receive an information society service' requested by the user (i.e. from the user's and not the organisation's perspective).

In addition, under Regulation 5(4) of the ePrivacy Regulations, consent must be given (and the information provided) in a way that is as 'user-friendly as possible'.

The Guidance – key takeaways

The Guidance augments this, seemingly simple, legal position. It is notable that it is significantly more detailed than the DPC's previous guidance, though not as detailed as the equivalent guidance given by the UK Information Commissioner's Office.

After explaining the law on cookies summarised above, the Guidance states that the purpose of the law on cookies is to protect individuals from having information placed on their devices, or accessed on their devices, without their consent, that may interfere with the confidentiality of their communications.

The Guidance also states that the law applies to any storage of information on a user's device or equipment, as well as to access to any information already stored on the equipment. Importantly, it is irrelevant whether the information stored or accessed consists of, or contains, 'personal data' — the ePrivacy Regulations still apply

regardless. However, organisations that do process personal data as part of their use of cookies need, in addition, to ensure that any such processing also complies with the GDPR and the Data Protection Act 2018. In addition, online identifiers (such as cookies) are included within the definition of personal data in Article 4(1) of the GDPR.

Consent generally

Arguably the most important aspect of the Guidance is that the DPC has clearly stated that consent for the setting of cookies (unless an exemption applies) is the GDPR standard of consent. This consent means a 'freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her'. The DPC's shorter cookies guidance document from 2019 effectively said the same thing, but the effect of this change on the law applying to cookies may not have been fully appreciated by all organisations to date.

One of the findings of the cookies sweep was that organisations set a lot of non-essential cookies before the consent of a user is sought. The DPC was critical of this in its report. The Guidance is clear that consent must be obtained for each individual purpose, and that consent cannot be bundled for multiple purposes at the same time. Similarly, the Guidance is clear that consent does not need to be given for each individual cookie, but, rather, that it must be given for each purpose for which cookies are used.

"Arguably the most important aspect of the Guidance is that the DPC has clearly stated that consent for the setting of cookies (unless an exemption applies) is a GDPR standard of consent. The DPC's shorter cookies guidance document from 2019 effectively said the same thing, but [this] may not have been fully appreciated by all organisations to date."

As with any other GDPR consent, a user must also be able to withdraw it as easily as they have given it. To enable this in practice, the Guidance recommends that information should be provided in the cookies information (in reality, a cookies policy) as to how users can later withdraw their consent to the use of cookies.

The Guidance notes specifically that any processing of special category data (e.g. health data) as part of a cookie's operation will require explicit consent. As a result, the DPC states, this high bar is unlikely to be met by means of generic information in a cookie banner or privacy policy. The DPC also takes the view that particular care has to be taken with cookies which obtain user location tracking information which must only be set with the user's consent (i.e. cannot be the subject of an exemption under the ePrivacy Regulations).

Cookie banners/ pop ups

Quite a number of website operators have chosen to use a cookie banner/pop-up to display that first layer of information, seek consent and provide a link to a cookies policy or similar for further information. At the moment, a number of those websites seek consent 'by implication' — e.g. that continued use of the website is deemed consent. The DPC is clear that consent cannot be obtained in this fashion — indeed this is an obvious outworking of the adoption of GDPR standard consent to the use of cookies (when compared to the pre-GDPR position). As such, the DPC's view is that cookie banners that simply disappear after further use of a website are not compliant, and do not indicate freely given and unambiguous consent.

The Guidance is also clear that use of pre-checked boxes, sliders or other tools set to 'ON' by default are not forms of validly obtained consent. Further, the use of a banner that merely gives the option to click 'accept', 'ok' or 'I understand', and which does not provide any option to reject cookies, or to click further for more detailed information is not, in the DPC's view, compliant.

Even when organisations have set up a cookie banner to obtain a clear consent to the setting of cookies, the Guidance is also very clear that those banners or pop-ups cannot be designed or set up in such a way as to 'nudge' a user into accepting cookies over rejecting them. Significantly, the DPC states that if an organisation uses a banner with an 'accept' option, it must give 'equal prominence to an option which allows the user to 'reject' cookies, or to one which allows them to manage cookies and brings them to another layer of information in order to allow them do that, by cookie type and purpose'. It is clear from this statement, however, that the DPC does not strictly require a binary accept/ reject to always be included for consent to cookies in all cases, and that it may, in theory, be acceptable, in place of 'accept'/'reject' option, to have an 'accept'/'seek further information' or 'manage settings' approach.

Obtaining a higher standard of consent can cause practical difficulties for organisations when setting non-essential cookies, as it can readily be appreciated that the positive acceptance rate of non-essential cookies (e.g. advertising cookies) is not very high on the part of users. As such, organisations, particularly those in the adtech space, may find it more challenging to try to implement a form of mean-

(Continued on page 6)

(Continued from page 5)

ingful informed choice for users while at the same time not unduly directing them towards 'accept' in all cases in an effort to maximise commercial returns.

As to the practicalities of obtaining consents, the Guidance notes the possibility of the use of 'consent management platforms' as a tool to do this, without mandating their use. These often appear to users as pop ups/ sliders to manage the seeking of cookie consents to different purposes. However, it is clear that any deployment of these tools is not itself a substitute for properly considering an organisation's use of cookies.

Information requirements

On any cookie pop-up/banner as the first layer of information, the Guidance is clear that organisations must at least provide information that allows the user to reject non-necessary cookies or to request more information about the use of cookies. In the second layer of information, which may be the organisation's cookies policy, the Guidance suggests that organisations must provide further information about the types and purposes of the cookies being set and the third parties who will process information collected when those cookies are deployed. The Planet49 case at the Court of Justice of the EU (*Bundesverband der Verbraucherzentralen und Verbraucherverbände - Verbraucherzentrale Bundesverband e.V. v Planet49 GmbH*, 1st October 2019) which also outlawed pre-checked boxes, requires that information be provided on the duration of the cookies.

The DPC reminds organisations that users must always be able to read cookies and privacy policies without any cookies (other than those falling into one of the two exemptions) being set and must be able to find those policies without them being obscured by anything else.

Timeframes

The Guidance takes the view that the expiry date of a cookie should be proportionate to its purpose (e.g. a shopping cart cookie should not have an indefinite expiry date). As to a timeline for consent, the DPC's view is that users should be asked to reaffirm their consent to cookies every six months. This can be done through use of a cookie to remember the consent, with such cookie being set to expire after that period. Beyond that six month period, the Guidance takes the view that a controller would need to objectively justify its use of cookies with a longer lifespan to record a user's consent state.

Third parties

Mindful of the CJEU judgment in the Fashion ID (*Fashion ID GmbH & Co.KG v Verbraucherzentrale NRW eV*, 29th July 2019 case), the Guidance notes that when using 'like' buttons, plugins, widgets, pixel trackers or social media-sharing tools which process personal data, organisations should be clear on what data are being sent to third parties, as well as of the fact that the organisation may also be considered a controller in respect of any personal data that it collects and discloses to those third parties.

Ultimately, the degree of responsibility of each party for determining the purposes and the means of the processing will dictate the relationship between the parties. As such, care should be taken to ensure that there is clarity on any cookies-based interactions with third parties, so that the data protection implications can be considered. As an example, merely including a social media sharing tool on an organisation's website may lead to a degree of responsibility for the data collected via that tool and processed by the third party.

In addition, the Guidance notes that any third parties processing personal data on behalf of the organisation arising from use of cookies will also have to be considered. Where this is the case, an appropriate data processing agreement between the organisation as controller and the third party processor will have to be entered into.

Cookies compliance roadmap

The DPC has allowed six months from April 2020 for organisations to assess, review and consider their existing cookies practices and, where necessary, to take action to bring these into compliance with the law. Once that period has elapsed, the DPC has stated that enforcement action may ensue against those entities which do not bring their cookies practices into compliance. Even though the law on cookies are set to be overhauled by a new European ePrivacy regulation, this is not finalised and it is clear that the DPC wishes to see the existing law complied with.

Given this, organisations now have a relatively short period of time in which to assess and rectify any issues with their operation of cookies in light of this new guidance.

The following steps might be of assistance in progressing any such exercise to improve compliance in this area.

Step 1: The first step in seeking to improve an organisation's cookie compliance is to undertake an assessment or audit, probably assisted by the organisation's IT team, to ascertain the current cookies and similar technologies which are used in the organisation's user facing websites, apps and similar. That review should consider and document each cookie, which organisation sets it (i.e. first or third party), the purpose for which it is set, any third party to which any relevant data is sent and the duration for which the cookie is set.

Step 2: Armed with that information, an assessment should be made as to whether or not any of the existing cookies could be removed from use or their duration modified, and whether any of the cookies are properly 'strictly necessary' from the user perspective (and as such can benefit from the exemption from consent).

Step 3: A suggested next step is to draft (or revise) a cookies policy for the organisation which sets out clear and comprehensive information about the types, purposes and duration of the cookies being set and the third

parties who will process information collected when those cookies are deployed. This should also explain how consent can be withdrawn.

Step 4: From that point, a (revised) cookie banner/pop-up could be designed and put in place. This would provide some clear initial information to allow an informed consent, point users to the cookies policy and seek consents to the different purposes of the cookies intended to be set. Best practice would suggests that users are given a clear and equally prominent choice between acceptance or rejection of each such type of cookie intended to be set, but organisations seeking to maximise non-essential cookie uptake might consider seeking to present an 'accept' and a 'manage settings' type option with equal prominence given to both options as a potential compromise. Whether this is acceptable might depend on the privacy intrusiveness or otherwise of the relevant cookies.

Step 5: Undertake some user testing of the newly adopted cookies consent approach to obtain user feedback and adjust accordingly.

Step 6: Where any cookies process personal data, ensure that any such processing is properly taken account of in the organisation's existing GDPR compliance framework. For example, an organisation should make sure that any relevant privacy policy/notice is updated and consistent with the cookies policy and seek to ensure that the organisation's Article 30 GDPR record of processing activities also clearly reflects the organisation's use of cookies.

Mark Ellis
McCann FitzGerald
Mark.Ellis@mccannfitzgerald.com