TECHNOLOGY

DPC Publishes Guidance on Cookies and Report on Cookie Sweep

16 April 2020

In this briefing, we consider the recent guidance of the Irish Data Protection Commission ("**DPC**") on the use of cookies and other tracking technologies ("**Guidance**") published on its website earlier this month.

The Guidance was issued on foot of the DPC's report on the findings of its "cookie sweep" – a thorough survey of the websites and practices of 38 well-known organisations across a range of sectors. In conducting the sweep, the DPC sought to examine how organisations are using tracking technologies, and to establish whether, and to what extent, organisations are complying with the prevailing law on cookies, being the European Communities (Electronic Communities Networks and Services) (Privacy and Electronic Communications) Regulations 2011 (S.I. No. 336 of 2011) ("**ePrivacy Regulations**") in respect of the use of cookies, and the General Data Protection Regulation (EU) (2016/679) ("**GDPR**") in respect of the processing of personal data via the cookies.

CONTEXT

It is a long-established requirement of the ePrivacy Regulations that organisations cannot place cookies on users' devices unless the user has been provided with "*clear and comprehensive information,*" and provided they have given their consent to the placement of such cookies. As we set out in our briefing on the Opinion of the European Data Protection Board ("**EDPB**") on the interplay between the ePrivacy Directive and the GDPR, cookie consent must meet the GDPR standard of "*consent,*" meaning that it must be freely given, specific, informed and unambiguous.

It would seem that regulators and organisations alike have been struggling to identify a solution that complies with the law while avoiding overly impinging on the user experience. Indeed, the guidance of supervisory authorities has been inconsistent across the EU, so much so that the EDPB has stated that it hopes to establish a common approach to cookie consents by working with different supervisory authorities. For organisations that have their main establishment in Ireland, it has been unclear which approach should be adopted, with many opting for "*no change*" in the absence of direct guidance from the DPC. Now that the DPC has issued guidance, organisations should not delay any longer in ensuring that their approach is compliant. Mere "cosmetic" changes are unlikely to suffice, and wholesale changes may be required by some organisations.

RESULTS OF THE COOKIE SWEEP

Based on the results of its sweep, the DPC concluded that many organisations may misunderstand what is of required of them. Twenty of the targeted organisations were given an "amber grading," indicating a good response and approach to compliance but signalling at least one serious concern. Twelve organisations were given a "red grading" due to poor quality responses, bad practices with cookie banners, setting cookies without consent, poor policies on cookies and privacy, and an overall failure to grasp the objectives of ePrivacy law. Only two organisations were given a "green grading," meaning that the DPC found them to be substantially compliant.

Some of the most common failings included the following:

- Implied consent for non-exempt cookies: many organisations displayed an over-reliance on implied consent disclaimers e.g. "by continuing to browse this site you consent to the use of cookies." Others relied on pre-ticked boxes, which are not permitted, as confirmed by the Court of Justice in the *Planet49* case. Some websites set non-essential cookies on landing without any user engagement.
- Labelling cookies as "necessary" or "strictly necessary" where they are not exempt: Consent is not required only where the use of the cookie is necessary "*for the sole purpose of carrying out the transmission of a communication over an electronic communications network,*" or where "*strictly necessary in order to provide an information society service explicitly requested by the user.*"
- Poor information on the use of cookies and their purposes.
- Badly designed cookie banners: many websites offered no choice other than "accept," without providing any additional information about the cookies.
- Bundling of consent for all purposes:

users were unable to provide specific consent to different cookie uses (e.g. necessary, analytics, marketing).

- Inability to vary or withdraw consent: the user interface of most websites had no obvious functionality to change settings or withdraw consent at a later stage. Under Article 7(3) of the GDPR, for consent to be "*freely given*" and therefore valid, users must be able to withdraw their consent to the processing of their personal data at any time.

In concluding that "*bad practices were widespread even among companies and controllers that are household names,*" the DPC has acknowledged that there are systemic issues that require its guidance, "*followed by possible enforcement action where controllers fail to voluntarily bring themselves into compliance.*"

MOVING FORWARD WITH THE DPC'S GUIDANCE

Obtaining Valid Consent

As consent must be "*freely given,*" websites should not "nudge" users to accept cookies by way of the design of a banner, a pre-ticked box etc. In this regard, the DPC has recommended the removal of pre-checked boxes from websites, and suggested that interfaces give the same prominence to a "reject" option as they do to an "accept" option. Given that consent must be "*unambiguous,*" and "implied consent" by scrolling a website or relying on browser settings will not suffice, the DPC has also advised that any cookie banners should not disappear in the absence of user engagement.

To ensure that specific consent is obtained to distinct cookie uses, and to enable the withdrawal of consent in accordance with Article 7(3) of the GDPR, the DPC recommends that organisations avoid bundling cookie consents (e.g. by forcing users to accept "all" marketing, analytics, tracking cookies etc.). Organisations should also provide information on how users can subsequently withdraw their consent to cookies, and provide them with a convenient mechanism to do so.

As consent must be "*informed,*" the DPC has further noted that swift changes are required to ensure that "clear and comprehensive information" about cookie use is provided to comply with Regulation 5(3) of the ePrivacy Regulations and to meet the transparency requirements of Articles 12-14 of the GDPR.

Retention Periods

Insofar as cookies retain personal data, data controllers cannot retain personal data for any longer than is necessary in accordance with the storage limitation principle under the GDPR. Although the legislation is silent on the appropriate lifespan of a cookie, the DPC has noted that it should be proportionate to its function. Based on a "first-principles analysis," the DPC has concluded that consent should be reaffirmed no later than six months after the user provided their consent, meaning that organisations should carefully check their current practices and seek new consents where required.

Consent Management

Users must be provided with a clear option to change their consent at any time, either by means of a settings tool or a so-called radio button. Many organisations have turned to consent management providers/platforms, who promise to assist organisations in managing consents and respecting users' preferences. However, the DPC has cautioned that the use of these tools does not in itself ensure compliance. The relevant tool "*must do what it purports to do*" and should not use pre-ticked boxes or toggle buttons that are unclear as to what is consent and what is not. The organisation must also maintain a record of users' consents to comply with its record-keeping requirements under Article 30 of the GDPR.

Joint Controllers

In the wake of the *Fashion ID* case, which we discussed in this briefing, the DPC has reminded organisations that they must assess their relationships with third parties whose tracking technologies and social media tools are deployed on their websites. Organisations must be aware of the data they are transmitting to third parties and note that they may be deemed a data controller (or a joint controller with the third party) in respect of that data.

On a somewhat related issue, the DPC has also reminded organisations that they must conduct a data protection impact assessment (a DPIA) if the use of cookies (or any of their operations) involve "*the combination, linking or cross-referencing of separate datasets where such linking significantly contributes to or is used for profiling or behavioural analysis of individual,*" noting that the need is more pronounced "*where the data sets are combined from different sources and where processing was/is carried out for different purposes or by different controllers.*"

Special Categories of Data

The DPC has also drawn attention to the difficulty in lawfully using cookies to process "special" categories of data under Article 9 of the GDPR. In most circumstances, the only available exemption for processing personal data relating to health, religion or sexual orientation etc. will be the "*explicit consent*" of users under Article 9(2)(a). In this regard, the DPC has noted that "*generic information in a cookie banner or privacy policy*" will not enable organisations to reach this high bar of explicit consent.

NEXT STEPS

The DPC has indicated that it will give organisations six months to consider its recommendations before engaging in any enforcement action under the Data Protection Act 2018. Interestingly, similar to the position adopted by the UK Information Commissioner's Office, the DPC has said that first-party analytics cookies are likely low risk and therefore are unlikely to be a priority for enforcement. What is clear however is that the DPC does intend to actively exercise enforcement powers later this year in the case of those websites and apps that do not significantly adjust their cookie consent management processes. Accordingly, while there may have been some merit to a "wait-and-see" approach in respect of the long-promised ePrivacy Regulation, this is no longer tenable, and organisations must take steps to comply with the law as it is, pending any agreement at EU level on the long-promised ePrivacy Regulation.

The authors wish to thank Sorcha McKendry for her contribution to this briefing.

KEY CONTACTS

Rob Corbet
Partner
+353 1 920 1211
rob.corbet@arthurcox.com

Ciara Anderson
Associate
+1 415 829 4247
Ciara.Anderson@arthurcox.com

Caoimhe Stafford
Associate
+353 1 920 1328
Caoimhe.Stafford@arthurcox.com