EDPB's guidance on consent — what's new?

Alex Jameson, Associate with Bates Wells, looks at the new changes in the EDPB's guidance on consent

In a development that could excusably have been missed, on 4th May 2020 the European Data Protection Board ('the EDPB') adopted its Guidelines 05/2020 on consent under the GDPR ('the Guidelines, copy at www.pdpjournals.com/docs/888092). The Guidelines are an updated version of those adopted by the EDPB's predecessor body, the Article 29 Working Party, on 10th April 2018. The majority of the content remains the same, with only editorial tweaks. In other words: no alarms and no surprises. However, the Guidelines provide clarity on two points of practice particularly relevant to the collection of consent for web cookies — something industry continues to grapple with two years after the GDPR coming into force. This article looks at the new clarifications and explains what they mean in practice.

Two changes

The new Guidelines contain only two substantive changes from the position set out in the previous version:

- clarity on the validity of consent obtained using 'cookie walls' — such consent is not valid; and
- more detail on the requirement for a clear and affirmative action, in particular in relation to 'scrolling and swiping' through a webpage – such activity does not suffice.

These novel aspects of the Guidelines are particularly relevant to cookie consent as required under the 2002 ePrivacy Directive for all but 'strictly-necessary' cookies. The standard of consent required under the ePrivacy Directive is that set out in Articles 4 and 7 of the GDPR.

Cookie walls

A 'cookie wall' is exactly what it sounds like: a barrier to accessing a website unless and until the user provides their consent to place cookies (so that the website can do things like collect analytics to track engagement, or monetise traffic with advertising cookies). Since 2018, cookie walls have been used by some as an attempted solution to certain problems website operators have had with obtaining GDPR-quality consent. For example, strictly speaking, users should be able to refuse their consent and consent should be obtained before cookies are placed on a user's device. However, many websites were simply not configured in a way that allowed a version to be presented without 'unnecessary' cookies. Consent via a cookie wall was therefore seen as a necessary condition of entry, the argument being that if a user did not want to give their consent, they were free to visit alternative websites.

The EDPB's position, clarified in the new Guidelines, is that consent collected via 'cookie walls' will not be valid, as the user is not presented with a genuine free choice and so that consent does not meet the requirement that consent be 'freely given'. The Guidance states that: "in order for consent to be freely given, access to services and functionalities must not be made conditional on the consent of a user to the storing of information, or gaining access of information already stored, in the terminal equipment of a user (so called cookie walls)".

This will be unsurprising to privacy practitioners, as it is consistent with the position taken by European data protection authorities including those in the Netherlands and France. In the UK, the Information Commissioner's Office guidance on cookies says that: "if your use of a cookie wall is intended to require, or influence, users to agree to their personal data being used by you or any third parties as a condition of accessing your service, then it is unlikely that user consent is considered valid." The EDPB's statement also complements the Court of Justice of the EU's judgment in the Planet49 case (C-673/17) in which an online gaming company sought users' consent to cookies by way of a pre-ticked box, and made the consent a condition of entering into a promotional lottery. Consent in that case was found by the court to be invalid.

It is clear, then, where EU Supervisory Authorities fall in the debate around the sanctity of privacy rights and their compatibility with the concept of a free internet. Some would argue that no access to a website is truly free; data is the price and always has been, and if data cannot be monetised, the model will need to change. *The Washington Post* has taken this approach, allowing users to turn off trackers and cookies for a monthly fee, or accept a free version of its website in return for consent to advertising cookies.

The ICO wrote to *the Washington Post* with a warning, but acknowledged that there was little more it could do in terms

of enforcement, given the *Post* is based in the US.

Swiping left on swiping and scrolling

For consent to be valid under the GDPR, it must be signified by a clear and affirmative action. The principle that passive behaviour, such as the continued browsing of a website, does not amount to a clear and affirmative action is not new. Indeed, the Article 29 Working Party confirmed this in its 2018 Guidelines when it said that: "Scrolling down or swiping through a website will not satisfy the requirement of a clear and affirmative action." The new Guidelines include an emphatic restatement of this principle, adding that such activity will not satisfy this requirement "under any circumstances". Additionally, the EDPB has provided the reasoning that:

- such actions are difficult to distinguish from other activity or interaction by the user (e.g. "oops, I was just trying to read the news and now I'm being profiled"), and are therefore too ambiguous; and
- it would be difficult to provide a way for the user to withdraw their consent as easily as they have given it (as is required under Article 7(3) of the GDPR).

The emphatic position taken by the EDPB (under any circumstance) is interesting. It seems to rule out the possibility for a mobile app to present a consent statement in such a way that would ask the user to 'swipe right if you consent, or swipe left if you do not'. However clear that action might arguably be, it would be too difficult to provide users with a 'swipe to withdraw consent' function. It is also unclear where other methods stand, such as clicking 'play' on a video or waving at a smart camera. Presumably, if sufficiently clear and prominent information was given before the opportunity to click play or to wave', this method could be made to satisfy the first requirement. However, it would likely fall afoul of the second, it being too difficult to withdraw consent in the same manner. And this guidance arguably further blends any distinction between the standards required of consent under Article 6 GDPR, and 'explicit consent' as a condition for processing special category data under Article 9 GDPR. It is clear that the regulators' approach to 'unambiguity' alone results in a very high standard for 'plain' consent, probably not far below that for explicit consent.

What did the old guidance say again?

Given the majority of the new Guidelines remain substantively the same as the version adopted by the Article 29 Working Party in 2018, as a reminder, some of the key points in that guidance are:

- consent should be granular – i.e. consent is potentially not valid where the controller has conflated several purposes, and has not attempted to seek separate consent for each;
- warning against 'click fatigue', or the impact of individuals receiving multiple consent requests every day;
- consent collected via browser settings is not ruled out, and many are hopeful that this will over time provide a solution to the cookie consent requirements, but in practice this may be difficult to obtain; and
- consent does not last forever and should be refreshed at 'appropriate intervals'.

Will the Guidance be enforced?

Whilst priorities may lie elsewhere at the moment, there is increasing pressure on EU Supervisory Authorities to flex their muscles. In April 2020, privacy browser company Brave lodged complaints with the European Commission against 28 EU Member States for under-resourcing their national data protection authorities (and we have seen the results of Max Schrems' privacy activism in the courts recently — goodbye, Privacy Shield!). Against this backdrop, a number of EU authorities including in Ireland, Belgium and France have warned that enforcement action is on the horizon.

Similar statements have been made by the UK ICO, but there is also an implication that the ICO is unlikely to prioritise enforcement where the perceived privacy intrusion is lower, such as consent for first party analytics cookies. And the ICO has recently paused its investigation into ad-tech and real time bidding in light of a reassessment of its priorities during the coronavirus pandemic.

What about the e-Privacy Regulation?

Whilst the regulators' position on consent under the GDPR is coalescing, the position as it pertains to cookies could change with the enactment of the proposed e-Privacy Regulation. The Regulation has been mired in delays and disagreements between Member States, and is unlikely to reach agreed form until 2021 at the earliest, after which it will need to pass through Trilogue negotiations among the European Parliament, European Council and the European Commission.

It is possible that the final e-Privacy Regulation will have an impact on the practice of cookie walls. An earlier draft of the Regulation appeared to condone them under certain conditions, stating that "making access to website content provided without [payment] dependent on the consent of the end user to the storage and reading of cookies for additional purposes would normally not be considered as depriving the end user of a genuine choice if the end user is able to choose between services… [etc.]." However, this text has been struck out in the latest version (dated March 2020), and it seems that the current draft does not permit cookie walls, but this does demonstrate the possibility of further twists and turns to come.

Alex Jameson
Bates Wells
a.jameson@bateswells.co.uk