Cookie consent and the GDPR: a recipe for disaster?

November 2018

This article first appeared in the Privacy Laws & Business UK Report, Issue 100 (November 2018).

The arrival of the GDPR has added another layer of complexity to an already difficult area of privacy law. It has also led to a multitude of different approaches to cookie consent. With that in mind, we look at what makes the law around cookies complex, and how it is often necessary to take a risk-based approach to obtaining cookie consent in a post-GDPR landscape.

What is a cookie, anyway?

A cookie is, at its most simple, a small file of information sent from a website to the user's device where it is stored as a basic text file. On subsequent visits to that website, the cookie will be automatically sent back from the user's device to the website's server. This enables the website to recognise the returning user.

Cookies can be set to expire at the end of a browsing session (session cookies), or can be stored in such a way that they remember the user and track their actions across the internet (persistent cookies). They can be set by the actual website you are visiting (first-party cookies), or indeed by a separate website or domain (third-party cookies). As well as different ways of setting cookies, there are also different types of cookies, which can be broken down into the categories set out in the "Categorising Cookies" box.

The data contained in a cookie can often be linked back to an individual, by identifying their internet protocol address, or being unique to a particular user's device. These so-called "cookie identifiers" mean that many cookies fall within the concept of personal data.

Categorising cookies

"**Strictly necessary**": Cookies that are strictly necessary to provide an "information society service" (e.g. an online service) requested by the user or subscriber. Examples include cookies which remember what is in a shopping basket, provide website security, or ensure a page loads smoothly.

"**Performance**": Cookies used to gauge user interaction and to aid website improvement (error management, site analytics, etc.).

"**Functionality**": Cookies that remember user preferences (region, language, payment methods, font size, etc.).

"**Targeting**": Persistent (i.e. permanent) cookies that collect browsing habits to build user profiles and facilitate targeted advertising etc.

Privacy concerns

Privacy concerns regarding cookies are based on the fact that certain cookies can be used to track a user's online activity. Such targeting cookies enable organisations to build commercially valuable browsing profiles of individuals. This facilitates personalised, targeted advertising. Amid these concerns, some organisations outside of Europe have even started geo-blocking access to their websites, in an apparent effort to prevent being caught by the GDPR's extra-territoriality provisions on the monitoring of individuals' behaviour.

Do all cookies raise privacy concerns?

In short – no. Cookies which are "strictly necessary" (see the "Categorising Cookies" box above) do not raise concerns (and should not require consent). It is the more intrusive cookies that have attracted the attention of regulators since the early 2000s, as opposed to strictly necessary, performance, or even functionality cookies. However, we are now in a position where, unless an exemption applies, the setting of cookies is only permissible with the GDPR-compliant consent of the website user/subscriber.

The legal framework

The EU's privacy landscape has evolved significantly over the past 15-or-so years to create a situation where the applicable rules and regulations surrounding cookies can be confusing and difficult to implement. The regulation of cookies in Europe first came to people's attention through the 2002 Privacy and Electronic Communications Directive (the so-called ePrivacy Directive), which set out the obligation to provide clear and comprehensive information about the purposes of the cookies being set, and the ability to opt out from cookies altogether.

The legislative timeline

2002	Original ePrivacy Directive adopted
2009	ePrivacy Directive amended to make cookie consent mandatory
2018	GDPR applies, strengthening consent requirements
2020?	New ePrivacy Regulation comes into force?

A shift to consent

The ePrivacy Directive was then amended by the 2009 Citizen's Rights Directive, which shifted from a position of informed opt-out to one of informed consent. While consent guidance from the Article 29 Working Party (endorsed and adopted by the European Data Protection Board (EDPB)) confirmed that website operators could not rely on implied consent, the UK's Information Commissioner's Office (ICO) moved away from that position. The ICO recognised that websites could in fact rely on implied consent, so long as that consent was still a specific, informed, direct expression of the user's agreement to the setting of cookies.

The impact of the GDPR

Although the ePrivacy Directive has always been the primary domain for the EU regulation of cookies, the implementation of the GDPR in May 2018 has added an extra layer of complexity. This is because consent under the ePrivacy Directive is defined by reference to consent under the EU's data protection regime.

As a result, when the GDPR replaced the Data Protection Directive, the GDPR's new (higher) definition of consent applied to the ePrivacy Directive. This means that, where required, cookie consent must now be freely given, specific, informed *and* unambiguous.

How has consent changed?

Pre-GDPR consent	freely given specific informed
GDPR consent	freely given specific informed unambiguous clear and affirmative

Some have argued that the GDPR concept of consent should not apply to cookies, because Article 95 of the GDPR (*Relationship with ePrivacy Directive*) prevents additional obligations being imposed by the GDPR where those matters are already subject to similar obligations in the ePrivacy Directive. However, regulators do not consider consent requirements to be an "additional obligation"; they are seen as preconditions for lawful processing.

So, in order for cookies that require consent to be used compliantly, websites must: (i) be transparent and tell people that the cookies are there; (ii) explain clearly what those cookies are doing and why; and (iii) get the user's unambiguous consent to store those cookies on their device (unless the cookies are exempt, of course). So far, so good. However, what seem at first sight to be three simple steps become, with closer scrutiny, complex rules which throw up a number of practical difficulties.

Practical difficulties of GDPR consent

The practical difficulties stem from trying to seek consent for cookies that satisfies the wide-ranging requirements of the GDPR, while avoiding website redesign and harm to the online experience. In addition, targeted digital advertising has proved to be a reliable source of revenue for many organisations, enabling users to freely access content they would otherwise have to pay for. Disrupting that setup is not an action many organisations are keen to take.

Prior consent

One of the most problematic requirements for valid consent is that it must be obtained prior to the actual processing. This is an issue for cookie technology because cookies are often set immediately upon an individual's arrival on the website. Helpfully, the ICO has in the past recognised that obtaining prior consent is difficult. However, it has also been clear that, where possible, cookies should be delayed until users have had the chance to understand (and make choices around) what cookies are being set. The consent guidance adopted by the EDPB is explicit in stating that consent must be given prior to the relevant processing (something it says is clearly implied, if not actually stated, by the GDPR).

As a result of the practical difficulties organisations face in obtaining prior consent, market practice is mixed. However, increasing numbers of organisations are looking to tackle the issue of consent timing head-on.

Unambiguous consent

The new GDPR requirement for consent to be unambiguous has also raised some practical challenges for cookies. Internet users in the EU are now all too used to dealing with discreet pop-up banners at the bottom of a website's landing page. The user is then often able to simply either close the banner, or continue browsing without any interaction with the banner at all. This "auto-accept" approach has a limited impact on a user's experience of a particular website, and may well be argued to be freely given, specific and informed. However, it is harder to show that it is unambiguous.

Valid cookie consent must involve some form of unambiguous positive act (such as ticking a box in a pop-up dialogue box), and recent ICO guidance confirms that consent must be more than simply continuing to use a website.

Interestingly, however, the ICO's own cookie consent box does refer to consent being given by a person continuing to use its website. The ICO also confirmed, in its last substantial guidance on cookies (pre-GDPR), that it would take a proportionate approach to enforcement, and that particular care should be taken to ensure clear and specific consent is obtained where privacy-intrusive cookies are being used (though it is unlikely the ICO website would use such cookies on its site).

Responses in practice

In response, some organisations have started taking an approach where the website displays a notice which prevents visitors fully accessing the website, unless: (i) the use of cookies is either consented to in its entirety; or (ii) the visitor has otherwise selected the types of cookies that they are willing to accept.

Forcing interaction with a cookie consent mechanism and including a choice of cookies would appear to be the approach that is closest to full compliance. However, that approach is difficult: the majority of cookie libraries do not easily support the purpose-based selection of cookies.

Lack of choice? Proceed with caution.

Choice is fundamental in consent being freely given. Indeed, the ICO advised in May 2018 that consent would not be freely given unless users are easily able to disable cookies (with the exception of those that are exempt, of course). As a result, forced opt-in must be used with caution.

It has been argued that websites which use a forced opt-in approach to deny access to users who choose to refuse to consent to any cookies are acting unlawfully. This argument is based on the fact that denying access deprives a user of any real choice.

The consent guidance adopted by the EDPB states that it must be possible to refuse consent without negative consequences and there will be certain websites in relation to which a denial of access to that site could cause serious detriment to the user (the claims website of a health insurer, for example). Similarly, organisations should refrain from using consent mechanisms that only provide an option for the user to consent (without any particular choices).

Striking a balance

When assessing the issues around cookies and consent, it is certainly important to carefully consider the privacy impact of a particular cookie on data subjects. While some cookies do pose a privacy risk, many do not.

The Council of the EU has explicitly recognised that cookies can be a legitimate, useful tool in the provision and assessment of an online service and we expect the ICO to continue taking a risk-based approach to enforcement, focusing on privacy intrusive cookies.

What does the future hold ?

ePrivacy: the wait goes on

The ePrivacy Directive is due to be replaced by the forthcoming (but seemingly endlessly delayed) ePrivacy Regulation. This is intended to sit alongside the GDPR and create a comprehensive body of law governing the processing and privacy of personal data (including cookies) within the EU. The European Commission's original proposal regarding the ePrivacy Regulation simply stated cookie consent requirements would be streamlined, with the new rules providing an easy way for users to accept or refuse cookies through the settings on their internet browsers.

Under the current draft, consent would still be required for the use of certain cookies, with similar exemptions for strictly necessary cookies or for certain types of analytics (although it is not yet clear whether third-party analytics platforms will also fall within an exemption).

It is unclear what the final ePrivacy Regulation will look like, or indeed when exactly it might come into force. There have even been suggestions that the new Regulation may never actually get off the ground, though EU institutions such as the European Data Protection Supervisor seem determined to keep its momentum going.

Browser settings to the rescue?

In relation to a continued move towards cookie consent being effectively managed through a user's browser setting, it remains to be seen where the ePrivacy Regulation will end up on this issue.

While the original draft stipulated that browsers would have to provide end users with information and choices regarding their privacy settings before the browser is installed, the latest suggested revisions to the Regulation move away from this position.

The Austrian Presidency of the EU has expressed concerns regarding the burden that this obligation could place on browsers and apps, and wants to discuss a proposal to delete the relevant article from the draft. It will be interesting to see whether the original move to allow internet users to effectively design the level of their online privacy will in the end be completely removed from the ePrivacy Regulation, or rather just watered down. At any rate, as mentioned above, there is still great uncertainty around when the ePrivacy Regulation will finally come into force. Even if the text for the Regulation can be agreed in the coming months, any implementation period would mean that it is unlikely to be in force before the beginning of 2020, at the earliest.

Conclusion

On paper, it is becoming clearer what is lawful and what is not when it comes to cookie consent in the EU. However, market practice is only very slowly falling into line with the GDPR.

This may be because, in the past, the ICO had always maintained that monetary penalties were unlikely, and that it would take a proportionate approach to enforcement. That said, we are expecting updated guidance from the ICO on the use of cookies in the near future, and it will be interesting to see the extent to which that guidance addresses the concerns set out in this article.

There is therefore ongoing uncertainty around the future regulatory approach to cookies compliance. In addition, there is the possibility of future legal action by individuals for the misuse of cookies, as well as increased scrutiny on internet privacy more generally.

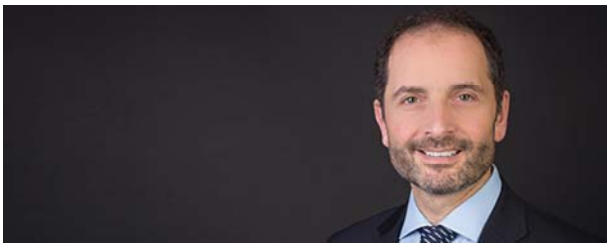
Earlier this year, many organisations took a risk-based approach to compliance by delaying tackling issues around cookie usage pending the arrival of the ePrivacy Regulation (rather than deal with it as part of a GDPR compliance programme). However, given the continuing delay of that Regulation, the period of non-compliance with the current ePrivacy Directive for those companies is increasing, which significantly changes the risk profile of this approach. Given this, it would be prudent for organisations to assess their own use of cookies, which will help in remaining well-placed to react to an ever-changing area of law.

This article was written by Rebecca Cousin, Rob Sumroy, Natalie Donovan and Duncan Mykura. Slaughter and May advises on all aspects of data protection and privacy. Please contact us if you would like any further information.

Further publications are available on our website.

Rebecca Cousin
T +44 (0)20 7090 3049
E rebecca.cousin@slaughterandmay.com

Duncan Mykura
T +44 (0)20 7090 3474
E duncan.mykura@slaughterandmay.com



Rob Sumroy
T +44 (0)20 7090 4032
E rob.sumroy@slaughterandmay.com

Natalie Donovan
T +44 (0)20 7090 4058
E natalie.donovan@slaughterandmay.com