ICO Cookies Guidance FAQs

Date : July 24, 2019

What is this all about?

Cookies or similar technologies are used by website operators to store or gain access to information stored on the device of an individual user. E-Privacy rules regulate the use of cookies and similar technologies (together "cookies") – in the UK these are set out in the Privacy and Electronic Communications Regulations 2003 (as amended, commonly known as PECR), which implement the EU E-Privacy Directive into UK national law. In addition, GDPR also applies to cookies.

In the UK the ICO is the regulator that deals with cookies and it recently issued its (revised) "Guidance on the use of cookies and similar technologies" ("the guidance") about how PECR (and GDPR, where applicable) apply to the use of cookies, which can be found here https://ico.org.uk/for-organisations/guide-to-pecr/guidance-on-the-use-of-cookies-and-similar-technologies/. These FAQs looks at key aspects of the guidance (i.e. it is not exhaustive of everything in the guidance, which is detailed and lengthy), especially consent which is very much the centerpiece about cookies and possibly the area of greatest risk for businesses.

What do the jargon terms about categorising cookies mean?

"Essential cookies" and "non-essential cookies":

- Essential cookies are cookies that are either, used only to carry out or facilitate transmitting communications over a network, or are strictly necessary to provide an online service which a user may have requested. Non-essential cookies are any cookies that fall outside this definition of essential cookies, for example cookies used to analyse a user's behaviour on a website or cookies used to display advertisements to a user.

"Session cookies" and "persistent cookies":

- Session cookies are cookies which expire at the end of a browser session, which is normally when a user exits their browser – they allow websites to recognise and link the actions of a user during a browsing session, for example to remember what a user has put in their shopping basket as they browse around a website. Cookies that can be stored for longer are called persistent cookies – they are stored on a user's device between sessions and can allow the preferences or actions of the user across a website to be remembered, for example to remember users' preferences and choices when using a website or to target advertising.

"First-party" and "third-party" cookies:

- First-party cookies are those set directly by the website the user is visiting, i.e. the URL displayed in the browser's address bar. Third-party cookies are set by a domain other than the one the user is visiting, which typically occurs when the website incorporates elements from other sites, such as advertising – when the browser or other software fetches these elements from the other sites they can also set cookies.

In a nutshell, what do the rules say?

PECR does not prohibit you using cookies. Instead, if you use cookies PECR requires you to:

- Say what cookies will be set;
- Explain what the cookies will do; and,
- Obtain consent to store cookies on devices.

What does the guidance cover?

The guidance covers the requirements for the use of cookies, focussing in particular on the two issues of transparency and consent.

What do I have to say about cookies?

Under the rules “clear and comprehensive information” must be provided about cookies – this relates to transparency requirements and the right to be informed (under GDPR). It means that when you set cookies you must provide the same kind of information to users as you would do when processing their personal data (and, as the guidance points out, in some cases your use of cookies will involve the processing of personal data anyway). The guidance says that this information has to cover:

- The cookies you intend to use; and,
- The purposes for which you intend to use them.

In addition, under the rules:

- You must make users aware of the cookies being placed on their devices; and,
- Your methods of providing this information, and the capability for users to refuse, are to be as user-friendly as possible.

As the guidance says, whilst providing information about cookies equates to transparency, levels of user understanding will differ – you will need to make a particular effort to explain cookies’ activities in a way that everyone can understand.

Long tables or detailed lists of all the cookies operating on a website are one possible way to present the information to users – this is increasingly popular. But, some websites might use a large number of cookies and therefore the guidance says that it may be helpful to provide a broader explanation of the way cookies operate and the categories of cookies in use; by way of example the guidance says that “a description of the types of things analytics cookies are used for on a website are more likely to satisfy the requirements than simply listing all the cookies you use with basic references to their function”.

How do I tell people about cookies?

The guidance says that in order to comply with the PECR information requirements you need to make sure users will see clear information about cookies (which will also increase levels of user awareness and control along with assisting in gaining valid consent). The guidance also states the following:

- You need to tell people about both the purposes and duration of the cookies you use;
- You need to provide information about cookies in such a way that the user will see it when they first visit your service, which is usually done within the cookie consent mechanism itself;
- You should also provide more detailed information about cookies in a privacy or cookie policy accessed through a link within the consent mechanism and at the top or bottom of your website; and,
- You should consider how the design of your online service impacts on the visibility of the link to your policy.

The guidance also suggests that other ways of increasing the prominence of cookie information include:

- Formatting – this might include changing the size of the link to the information or using a different font. The key is whether the link to this important information is distinguishable from “normal text” and other links;
- Positioning – simply moving the link from the footer of the page to somewhere more likely to catch attention is an easy but effective thing to try; and,
- Wording – making the hyperlink more than simply “privacy policy”; this could involve a link through some explanatory text, for example “Find out more about how our site works and how we put you in control.”

As the guidance says, all the while you need to ensure that the information is clear so that your users understand it – tailor the language to your audience and avoid using lengthy and overly complex terminology, i.e. keep it all simple and straightforward.

What about consent?

Consent is a key issue with regard to cookies and the guidance has a lot to say about this. Under PECR, users or subscribers are required to consent to cookies being placed or used on their device. Now it is the all-important GDPR definition of consent that applies to cookies, namely:

- "'consent' of the data subject means any 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."

Remember that GDPR also provides the following further specifics about consent requirements:

- You must be able to demonstrate that you have valid consent**;**
- Your consent requests must be clearly distinguishable from other matters;
- Your consent requests must be in an intelligible and easily accessible form, using clear and plain language; and,

- Your consent mechanism must allow the individual to withdraw their consent at any time.

GDPR also specifically bans pre-ticked boxes – silence or inactivity does not constitute consent. Under the guidance, with regard to cookies, this means that:

- The user must take a clear and positive action to give their consent to non-essential cookies – continuing to use your website does not constitute valid consent**;**
- You must clearly inform users about what your cookies are and what they do before they consent to them being set;
- If you use any third party cookies, you must clearly and specifically name who the third parties are and explain what they will do with the information;
- You cannot use any pre-ticked boxes (or equivalents such as "on" sliders) for non-essential cookies;
- You must provide users with controls over any non-essential cookies, and still allow users access to your website if they don't consent to these cookies; and,
- You must ensure that any non-essential cookies are not placed on your landing page (and similarly that any non-essential scripts or other technologies do not run until the user has given their consent).

How should I request consent in practice?

It's up to you. When considering how to provide information about cookies and how to request consent there are different techniques you can use to draw users' attention to information and the choices available to them. But, the guidance highlights the need to ensure that any consent mechanism you put in place allows users to have control over *all* the cookies your website sets and not just your own.

Can I use message boxes and similar techniques?

Yes, if done properly. Whilst message boxes such as banners, pop-ups, message bars, header bars or similar techniques might initially seem like an easy option, you need to consider their implementation carefully, particularly in respect of the implications for the user experience. By way of example and caution, the guidance says that "a message box designed for display on a desktop or laptop web browser can be hard for the user to read or interact with when using a mobile device, meaning that the consents you obtain would be invalid."

At the same time, the guidance stresses that GDPR is clear that electronic consent requests must not be unnecessarily disruptive and "so you need to consider how you go about providing clear and comprehensive information without confusing users or disrupting their experience", albeit whilst not "overriding the need to ensure that consent requests are valid" and "so some level of disruption may be necessary".

Can I rely on settings-led consent?

Yes. Some cookies are deployed when a user makes a choice over a website's settings. In these cases, consent could be sought as part of the process by which a user confirms what they want to do. By way of example, the guidance says that "some websites 'remember' which version a user wants to access, such as a version of a site in a particular language [sometimes called "preference cookies"]. […] If this feature is enabled by the storage of a cookie, then this should be explained to the user, meaning they needn't be asked every time they visit the site. You can explain to them that by allowing their choice to be remembered they are giving consent to set the cookie. Agreement for the cookie could therefore be seamlessly integrated with the choice the user is already making. This would apply to any feature where the user is told that a website can remember settings they have chosen".

But, the guidance also stresses that care must be taken "that any processing of personal data related to the setting of preference cookies or other personalisation features is limited to what is necessary for this purpose".

Can I rely on browser settings and other control mechanisms?

Not for now. The guidance says that it can't be assumed "that each visitor to your online service can configure their browser settings to correctly reflect their preferences in relation to the setting of cookies."

Under PECR, browser settings may be one means of obtaining consent if they can be used in a way that allows the subscriber to indicate their agreement to cookies being set, where the user sets up their browser so that only certain cookies are allowed. But, the guidance stresses that "not everyone accessing websites will do so with the same version or type of browser, or even use a traditional web browser at all."

The guidance says that in the "future you may well be able to rely on the user's browser settings as part, or all, of the mechanism for satisfying yourself that you have consent to set cookies. For now, relying solely on browser settings will not be sufficient. Even when browser options are improved it is likely not all users will have the most up-to-date browser with the enhanced privacy settings needed for the settings to constitute an indication of consent."

Can I use "terms and conditions" to gain consent for cookies?

No. Consent must be separate from other matters and cannot be bundled into terms and conditions or privacy notices. Consent must be obtained by giving the user specific separate information about what they are being asked to agree to and providing them with a way to accept by means of a positive action to opt-in.

Can I use "cookie walls"?

Not if this is a condition of service access. A so-called "cookie wall" (sometimes also called a "tracking wall") requires users to "agree" or "accept" the setting of cookies before they can access an online service's content, i.e. take it or leave it. According to the guidance, in some circumstances this approach is inappropriate such as where the user has no genuine choice but to sign up (under GDPR consent must be freely given) – "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".

Can I pre-enable any non-essential cookies?

No. According to the guidance, just because users may be unlikely to select a particular non-essential cookie when given the choice, or because the cookie is not privacy intrusive, is not a valid reason to pre-enable it. Enabling a non-essential cookie without the user taking a positive action before it is set on their device does not represent valid consent.

Typically a website may set non-essential cookies on its landing page and its cookie consent mechanism including wording such as "By continuing to use our website, you consent to our use of cookies". According to the guidance this does not represent valid consent, even if the mechanism also includes an "OK" or "Accept" button – this is because the website has decided non-essential cookies will be set, and is then seeking the user's agreement afterwards, but is only providing the user with an option to “continue” rather than a genuine free choice about whether the user wants to accept or reject the cookies.

According to the guidance, “A consent mechanism that emphasises ‘agree’ or ‘allow’ over ‘reject’ or ‘block’ represents a non-compliant approach, as the online service is influencing users towards the ‘accept’ option”. Further, “A consent mechanism that doesn’t allow a user to make a choice would also be non-compliant, even where the controls are located in a ‘more information’ section.”

What about cookies set on websites that mine links to?

Users could have cookies set during their interactions with you elsewhere, for example if you have a presence on social media platforms those platforms will set cookies on users’ devices once they visit your pages there, such as after they’ve navigated away from your website. These cookies can be used for different purposes depending on the platform, but common uses are to provide you with statistical information about how users interact with your social network presence.

Although you may not directly control the cookies that the platform sets, you do control the fact that you have a presence on that platform and you are also able to determine what types of statistics you want the platform to generate based on user interaction. According to the guidance, this means that you are jointly responsible, with the social media platform, for determining the purpose and means of the processing of personal data of any user that visits your presence on that network and are therefore a so-called “joint data controller” for this activity with the platform.

Not all of those accessing your social media presence from your website will necessarily be logged-in users of the social platform in question and therefore you need to ensure that they are provided with appropriate information before they visit. So, you need to ensure that your own privacy notice on your website includes references to any social media presence that you may have, and how individuals are able to control the setting of any non-essential cookies once they visit there, even if these cannot be covered by your site’s consent mechanism. You should also provide information about the processing of any personal data within your privacy notice as well as somewhere your page on the online platform, even if this is simply a link back to that privacy notice.

What if I use third-party cookies?

The guidance stresses that this is one of the most challenging areas in which to achieve compliance with PECR. Where your website sets third-party cookies, both you and the third party have a responsibility for ensuring users are clearly informed about cookies and for obtaining consent. The guidance acknowledges that in practice it is much more difficult for a third party to achieve this (as they have less control on the interface with the user) but also points out that users are likely to address any concerns or complaints they have to the person they can identify or have the relationship with, i.e. you, as the organisation running the website.

You and a third-party will likely need to engage constructively on the issue of your website allowing or using third-party cookies. Whilst the process of getting consent for third-party cookies will in particular be complex and challenging, as the guidance stresses, if your online service allows or uses third-party cookies you still have to ensure you provide appropriate information to users and that you are allowing them to consent to what is stored on their device.

What should I do about withdrawal of consent?

You should ensure that your consent mechanism has the technical capability to allow users to withdraw their consent (at any time) just as easily as they gave it. You must also provide information about how cookies that have already been set can be removed, for example in your consent mechanism or within your privacy or cookie policies. The consequences of withdrawing consent could be made clear, for example by explaining the impact on the functionality of the website.

How often should I get consent?

You may need visitors to consent again to cookie settings. A number of factors will be involved such as the frequency of visits or updates of content or functionality.

How long should my cookies last?

Whilst this depends very much on the purpose you use the cookie for, according to the guidance, ultimately you need to ensure that your use of the cookie is proportionate in relation to your intended outcome and limited to what is necessary to achieve your purpose – this is likely to lead you towards a determination of the duration. By way of example of clear cases where the duration of a cookie is wholly disproportionate the guidance says that "whilst it may be technically possible to set the duration of a cookie to '31/12/9999' this would not be regarded as proportionate in any circumstances.

Are there any exemptions to providing information and getting consent?

Yes, there are two exemptions, known as the "communication" exemption and the "strictly necessary" exemption. The communication exemption is about the transmission of a communication over an electronic communications network – for a communication to take place over a network between two parties certain conditions must apply. The strictly necessary exemption is about a service delivered over the internet where storage of (or access to) information should be essential rather than reasonably necessary. These exemptions are quite technical and not necessarily easy to apply, and therefore beyond the scope of further examination in these FAQs – it is recommended that proper technical and legal advice is sought if these exemptions are being considered.

What about enforcement?

In the guidance the ICO makes it clear that it will enforce compliance and "where organisations refuse or fail to comply voluntarily the ICO has a range of options available for taking formal action where this is necessary."

Where the ICO does consider formal action, for example where an organisation refuses to take steps to comply or has been involved in a particularly privacy-intrusive use of cookies without telling individuals or obtaining consent, the ICO says that "any use of formal regulatory powers would be considered in line with the factors set out in the ICO's Regulatory Action Policy" (for this document see here: https://ico.org.uk/media/about-the-ico/documents/2259467/regulatory-action-policy.pdf). According to the ICO, this policy document "makes clear that any formal action must be a proportionate response to the issue it seeks to address and that monetary penalties will be reserved for the most serious infringements of PECR". Importantly, the guidance states that:

- "[…] it is unlikely that priority for any formal action would be given to uses of cookies where there is a low level of intrusiveness and low risk of harm to individuals. The ICO will consider whether you can demonstrate that you have done everything you can to clearly inform users about the cookies in question and to provide them with clear details of how to make choices".

What are the takeaways?

The two key actions that businesses can do for now to review their cookies compliance are as follows:

- Check your existing cookies policy and amend it as appropriate; and,
- Check your consent mechanisms and revise them as necessary.

The guidance provides a more detailed breakdown of actions to take in the section entitled "How should we conduct a cookies audit?".

Under the proposed EU E-Privacy Regulation changes will be made to the existing EU rules about cookies, which we have written about here: https://www.corderycompliance.com/proposed-eu-e-privacy-regulation/. But, as the guidance emphasises until this proposal is fully agreed and comes into force, PECR will continue to apply in full, alongside the GDPR.

For more of our reporting about data protection issues see here http://www.corderycompliance.com/category/data-protection-privacy/.

Data breaches are also a key issue for organisations who need to make sure that they do all that they can to stop data breaches including ensuring they can react to data breaches quickly when they happen. Cordery's Breach Navigator can help organisations respond to a breach. There are more details here https://www.corderycompliance.com/solutions/breach-navigator/.

For more information about GDPR please see details of Cordery GDPR Navigator here www.bit.ly/gdprnav.

For more information please contact André Bywater or Jonathan Armstrong who are commercial lawyers with Cordery in London where their focus is on compliance issues.

André Bywater

Office: +44 (0)207 075 1785

andre.bywater@corderycompliance.com

Jonathan Armstrong

Office: +44 (0)207 075 1784

jonathan.armstrong@corderycompliance.com