

Despite the widespread awareness of the need to obtain “opt-in” consent for marketing emails (resulting in clogged-up inboxes during the run-up to the GDPR for many of us!), the need to apply the same standard of consent when setting website cookies appears to have escaped the notice of most online businesses in the UK. Many websites have continued to rely on implied consent to set cookies, by using a cookie notice which states that “by continuing to browse the site” the website visitor consents to the use of cookies or similar wording.

It was only a matter of time before the UK regulator, the ICO, clamped down on the continued use of implied consent for cookies post-GDPR, which cut against both [its own guidance on GDPR consent](#) and Article 29 Working Party's (WP29) guidance¹. Last week the ICO did just that, making it clear on its [blog \(“Cookies – what does ‘good’ look like?”\)](#) that sites that rely on implied consent to set cookies are not compliant with the GDPR consent standard that now must be read into the PECRs (see below for details), and publishing [new guidance](#) on the use of cookies.

In order to lead by example, the ICO also changed its own cookie notice on its website, so that it now requires the website visitor to proactively “turn on” the “optional” analytics cookies, with the default setting set to “off” for all but essential cookies.

What this means, in practice, is that every online business in the UK which currently relies on implied consent to set cookies needs to change its cookie notice and its procedures in line with the ICO's revised notice, to require the website user to positively opt-in to any non-essential cookies being set on their device. This new notice must, of course, be supported by underlying technology which ensures that the non-essential cookies are not set on a user's device unless and until they have positively consented.

Further detail on the cookie consent requirements is provided below.

What Are Cookies?

Alas, we are not talking about the baked goods that so perfectly complement a hot beverage. Cookies are small computer files that can be stored on a user's device when they are browsing a website. Cookies are used by website operators and third party ad tech firms for a variety of reasons, such as to track website traffic, to remember the content of your online shopping basket or for online advertising.

Cookies and Consent

In the UK, the Privacy and Electronic Communications Regulations 2003 (PECRs) regulate the use of cookies and similar technologies. These regulations were enacted by Parliament to implement the EU ePrivacy Directive² and similar regulations are in force throughout the European Union. The PECRs require the company setting the cookies to provide website users with clear and comprehensive information about the use of cookies and to obtain their consent to set them on their device. These requirements are commonly satisfied by providing a cookie banner, which tells the website user that cookies are set when they access the site and purports to obtain their consent to this, and a link to a cookie policy which provides more detailed information about the cookies to be set.

The GDPR, which came into force on 25 May 2018, set a stricter standard of consent for the use of personal data compared to the previous data protection law, because the GDPR requires consent to be specific, informed, freely given and provided by way of a positive “opt-in” by the individual. The GDPR standard of consent applies (through incorporation by reference) to the cookie placement consent obligation under the PECRs.

This obligation only applies to “non-essential” cookies. Consent is not required for the use of “strictly necessary” cookies, which are those that are essential to provide an online service which has been requested by the user. This criteria is interpreted strictly by the ICO. A cookie that is beneficial to the services provided by a website operator, but which is not an essential requirement for operation of the website, will not be classed as an “essential” cookie.

The ICO has made it clear in its new guidance that cookies that are necessary to comply with data security obligations or to remember goods which the user has placed into an online shopping basket will be classed as “essential” cookies, but analytics cookie will not, although, for first party cookies, the ICO has indicated that it will not prioritise enforcement of the rules. Cookies used for online advertising are not exempted.

The consent requirement for the placement of non-essential cookies on an EU website visitor's device should not be confused with the lawful basis for processing the various types of personal data that are collected from the cookie or other tracking application. The GDPR makes clear that the legitimate interests test may apply to such processing by the website operator and third parties, provided that the rights of the individuals whose data is being collected do not override those interests. Obviously, however, if consent is not provided for the placement of the cookie in the first place, the question as to the lawful basis for processing becomes a moot point.

¹ Guidelines on Consent under Regulation 2016/279 endorsed by the European Data Protection Board.

² Directive 2002/58/EC.

The Recent ICO Guidance on Consent – A Positive Act

The ICO's new Cookie Guidance makes it clear that cookie consent must be obtained by a positive action by the website user to show that they consented to the use of cookies, such as ticking a box, clicking a button or using a slider. Furthermore, pre-ticked boxes, cookies set to "on" as a default or other equivalents will not suffice as a positive act.

The guidance also makes it clear that non-essential cookies should not be set on the landing page of the website, until and unless the website user has positively consented to this. The need to obtain informed consent before the cookie is set was made clear by the WP29 as early as 2012 in its Cookie Consent Exemption opinion³. However, up until now, the ICO has taken a somewhat more relaxed approach to the timing of the consent.

The ICO's new guidance states that a website visitor must not be prevented from accessing the site on the grounds that they do not consent to the use of non-essential cookies. This means that so-called "cookie walls", which have been the subject matter of recent complaints against IAB Europe filed by Brave, will not be allowed in most cases.

Enforcement by the ICO and Beyond

It is no coincidence that the ICO's new cookie guidance has been published less than two weeks after it published its Adtech Update Report⁴, in which it examined the complex data privacy issues raised by programmatic advertising, concluding that there was a general lack of awareness of (and compliance with) the rules within the industry. The ICO has given notice that it intends to intervene in the market and it has given the industry six months to start to make the necessary changes.

The ICO's clamp-down on cookies is likely to be echoed across the European Union, with new cookie guidance expected from the French Supervisory Authority, the CNIL,⁵ this month and other supervisory authorities likely to follow suit.

Many websites in the UK are likely to be in breach of the cookie consent rules as clarified by the ICO last week, and it will take time for businesses to make the notice, process and technical changes required to comply, including ensuring that they have the technology to enable website users to pick and choose the cookies they agree to. In the final paragraph of its blog post, the ICO appears to recognise this, with a (gentle) word of warning:

"Cookie compliance will be an increasing regulatory priority for the ICO in the future. However, as is the case with all our powers, any future action would be proportionate and risk-based."

The ICO advises:

"...Start working towards compliance now – undertake a cookie audit, document your decisions and you will have nothing to fear."

Please get in touch with one of the contacts listed or any other member of our global Data Privacy & Cybersecurity team for further advice on this (or any other data privacy) topic, as well as practical compliance recommendations, including user-friendly off-the-shelf software applications.

Contacts

Rosa Barcelo

Partner, Brussels
E rosa.barcelo@squirepb.com
T +322 627 1107

Francesca Fellowes

Director, Leeds
E francesca.fellows@squirepb.com
T +44 113 284 7459

Eleanor Dodsworth

Trainee, Leeds
E eleanor.dodsworth@squirepb.com
T +44 113 284 7246

³ Opinion 04/2012 on Cookie Consent Exemption adopted 7 June 2012.

⁴ Update Report into Adtech and real time bidding – 20 June 2019.

⁵ Cnil.fr.