Cookie Policy

Article 5(3) of the *E-Privacy Directive (2002/58/EC)* clarifies that clear and comprehensive information should be provided in accordance with the *Data Protection Directive (95/46/EC)* (now repealed and replaced by the GDPR).

Online providers must therefore provide a clear, comprehensive and visible notice on the use of cookies, which complies with the GDPR's transparency requirements - the ICO Cookies Guidance confirms that this applies whether or not they are processing personal data. The information must be provided at the time and place where consent is sought, for example, via a banner on the first page that the user sees.

The transparency requirements also apply to cookies set by third parties on the online provider's service, for example, cookies, pixels and web beacons and any other methods of storing or accessing information including those from other services like, adtech providers or social media platforms (see *Working with third-party advertising providers*).

As user understanding levels will differ, the information should be sufficiently full and intelligible to allow individuals to clearly understand the potential consequences of allowing storage of a cookie and access to the information it collects. Online providers and their partner organisations need to be confident that their users have a shared understanding about what is likely to happen on the web pages that they visit (see *Who should obtain consent?*).

The WP29 *Working Document (02/2013) providing guidance on obtaining consent for cookies* says that organisations must provide users with "all necessary information" about cookies, including:

- The cookies used and their purposes.
- Any third-party cookies or third-party use of information (where the cookies are personal data in order to comply with the GDPR, third parties will need to be specifically named).
- Retention periods, that is, cookie expiry dates (for third-party cookies, this obligation could be met by linking to the third party's website, if the information is available there).
- Typical cookie values.
- Other relevant technical information.
- Information about how to accept all, some or no cookies and how to change the preferences in the future.

On 1 October 2019 the ECJ ruled in *Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband eV v Planet49 GmbH (Case C-673/17) EU:C:2019:801* (Planet49) that Article 5(3) of the E-Privacy Directive "must be interpreted as meaning that the information that the service provider must give to a website user includes the duration of the operation of cookies and whether or not third parties may have access to those cookies" to ensure that users give their informed consent (see *Legal update, Preliminary ruling that cookie consent must be active and specific (ECJ)* and *Blog, Crunch time for cookies?* and *Separate consent for different processing operations*).
Technically, there are many different ways in which to provide the information and the ICO and the WP29 both encourage creativity. Practically, a layered approach comprising a cookie banner (or a pop-up, a message bar, header bar or similar) and a Cookie Policy are frequently used to impart information and gain consent. For further information see *GDPR transparency and how can consent to cookies be validly obtained?*.

Consent requirements:

PECR requires that users or subscribers consent to cookies being placed or used on their device. The provision which introduced this requirement is regulation 5(3) of the *E-Privacy Directive (2002/58/EC)* (as revised by the *Citizens' Rights Directive (2009/136/EC)*). This provision states that: "… the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user has given his or her consent".

Regulation 6 of PECR implements regulation 5(3) of the E-Privacy Directive into UK law.
The rule applies to the storage of any information (unless an exemption applies) and is not dependent on the data being personal data (see *Limited exemptions to information and consent requirements*).

Neither the E-Privacy Directive nor PECR provide a definition of consent. Since 25 May 2018, the standard of consent has been set to that required by Articles 4(11) and 7 of the GDPR (see *What is valid consent under the GDPR?*).

Is legitimate interests a valid lawful basis for the placing of a cookie instead of consent?

No. According to the ICO, commenting more generally in the context of direct marketing and in its Cookies Guidance, if consent is required under *PECR* then, in practice, consent will also be the appropriate lawful basis under the *GDPR*. On this basis, as PECR requires consent to the placing of cookies, legitimate interests will not suffice.

The ICO's blog: Cookies – what does 'good' look like? of 3 July 2019 confirms that "PECR always requires consent for non-essential cookies, such as those used for the purposes of marketing and advertising. Legitimate interests cannot be relied up on for these cookies" (see *Legal update, ICO publishes new cookies guidance*).

The ICO recognises that an alternative lawful basis such as legitimate interests may apply for associated processing of personal data. This means that unless an exemption from PECR applies, consent will be required for the placing of the cookie. However, an organisation may be able to rely on legitimate interests for the subsequent processing of the data that was collected from the cookie. For example, consent will be needed for the placing of tracking cookies, but an organisation may be able to rely on legitimate interest for the subsequent segmentation of users an interest categories based on the cookie data (see *Limited exemptions to information and consent requirements*).

However, legitimate interests has its limitations and as the WP29 notes in its *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679*, adopted in October 2017 (WP251):"it would be difficult for controllers to justify using legitimate interests as a lawful basis for intrusive profiling and tracking practices for marketing or advertising purposes, for example those that involve tracking individuals across multiple websites, locations, devices, services or data brokering"

For further information see *Practice note, Overview of GDPR: UK perspective: Legitimate interests condition* and *ICO Guide: Legitimate interests under the GDPR*.

What is valid consent under the GDPR?

In May 2018, the ICO confirmed that the *GDPR* definition of consent applies to *PECR* (see *ICO: Consent under the GDPR* and *ICO: The rules around business to business marketing, the GDPR and PECR*). With effect from 29 March 2019 regulation 8(2) of the *Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 (SI 2019:419*) amended PECR 2003 to recognise in law that "consent" by a user or subscriber corresponds to the GDPR standard of consent (as defined in section 3(10) of the DPA 2018).

The GDPR defines consent as "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she by statement or by a clear affirmative action signifies agreement to the processing of personal data relating to him or her" (*Article 4(11)*). In particular, the ICO Cookies Guidance notes that:

- Consent requests must be accessible and in clear and plain language (Article 7, GDPR). Merely continuing to use the website does not constitute valid consent (see *Unambiguous consent*).
- Pre-ticked boxes are banned and silence and inactivity do not constitute valid consent (recital 32, GDPR) (see *Legal update, Preliminary ruling that cookie consent must be active and specific (ECJ)* and *Blog, Crunch time for cookies?*).
- Consent must not be "bundled" into terms and conditions or privacy notices (Article 7, GDPR).
- Individuals must be aware of the identity of any controllers relying on consent, so third parties must be named and an explanation of what they will do with the information must be provided (see *Naming third parties*).
- Cookie walls used as a blanket approach to restrict access to a service until a user consents will not constitute valid consent – users must still be able to access a website even if they don't consent to cookies (see *Can access to a website be made conditional on accepting cookies?*).
- Users must be provided with controls over any non-essential cookies.
- The consent mechanism must allow the user to withdraw their consent at any time (Article 7, GDPR).
- Non-essential cookies must not be placed on the landing page until the user has given their consent (see *When must consent to cookies be obtained?*).
- Organisations relying on consent must be able to demonstrate consent (Article 7, GDPR) (see *Demonstrating consent*).

(*Articles 4(11) and 7 and recitals 32, 42 and 43, GDPR*.)

Unambiguous consent

The consent section of the ICO's Guide to the GDPR notes that: "Consent should be obvious and require a positive action to opt in. Consent requests must be prominent, unbundled from other terms and conditions …"

A request for consent must, therefore, be separate from Terms and Conditions (see *ICO: Guide to the General Data Protection Regulation (GDPR): Lawful basis for processing: Consent*).

The ICO Cookies Guidance, the *WP29 Consent Guidance* and the *ICO Consent Guidance* are helpful in establishing what constitutes valid consent. To be valid, consent must be signified by some kind of positive action (for example, by clicking "I Accept" on the cookie banner or clicking a link or by picking preferences on a settings list or similar).

Inferring implied consent through inaction is insufficient to satisfy the GDPR. According to the WP29 Consent Guidance, a cookie banner should be implemented, and cookies should not be set or read until a user has taken some form of positive action. Further, it makes clear that merely continuing the ordinary use of a website alone (for example, by scrolling down or swiping through) is not

conduct from which valid consent can be inferred. Accordingly, online providers may find that the simplest and most transparent solution is to ensure that the consent involves clicking "I accept".