Digital advertising guidance:

cookies, consent and the GDPR

IAB UK
March 2020

Contents

1. About this guidance

IAB UK has produced this guidance as part of our commitment to provide responsible companies in our remit with standards and tools to facilitate legal compliance, responsible data use, and to ensure accountability, i.e. by setting out examples of what may be appropriate legal and technical approaches to achieving compliance with the General Data Protection Regulation (GDPR) and ePrivacy legislation (while recognising that individuals companies remain accountable for deciding what approaches they should take in practice).

The purpose of this guidance is to help educate the digital advertising industry about the legal requirements relating to the use of cookies and other similar technologies in the UK, to help companies understand their obligations, and how to comply with them in practice.

This guidance is intended as a high-level overview for companies engaged in digital advertising in the UK, based on relevant UK law. It does not constitute legal advice. Companies remain responsible for their own compliance with applicable laws, and should take their own legal advice where necessary.

We recommend that if you use cookies or other similar technologies for any purpose you review your practices and ensure that you are operating in line with the current, relevant legal requirements. If you have not reviewed or updated your approach to consent (e.g. your cookie notices on your website) following the introduction of the GDPR, you should do so.

About the ICO

The Information Commissioner's Office (ICO) is the UK's data protection and privacy regulator. It is responsible for enforcing regulation 6 (the particular regulation addressed in this guidance) of the Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR), and the GDPR in the UK.

Specifically in relation to the GDPR, the ICO regulates any:

- UK-established data controllers and processors (subject to the one-stop-shop mechanism where that entity has a main establishment elsewhere in the EU) and
- entities outside the EU that process the data of individuals in the UK.

The ICO has a comprehensive set of guidance and resources for organisations on data protection and the GDPR, available at https://ico.org.uk/for-organisations/. For information about the impact of Brexit from a data protection perspective see the ICO's website: https://ico.org.uk/for-organisations/data-protection-and-brexit/.

The ICO Update report into ad tech and RTB

In June 2019, the ICO published its 'Update report into ad tech and RTB' (the 'Update report'), which summarised the findings of its review of the use of personal data and cookies (and other similar technologies) in the real-time bidding (RTB) process. In its report the ICO set out its observations about RTB with respect to the relevant provisions of the GDPR and the Data Protection Act 2018, and PECR.

One of the six key points in the ICO's Update report was the use of legitimate interests for placing and/or reading a cookie or other similar technology (rather than obtaining the consent that PECR requires). We recommend that you read the Update report and familiarise yourself with the ICO's guidance on cookies (see section 5).

This guidance forms part of the actions set out in IAB UK's response to the Update report.

2. Cookies and consent

What you need to know

Background

In the UK, the use of cookies and other similar technologies is regulated by the 'ePrivacy Directive', implemented in the UK through the 'Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR)' (as amended)[1]. Where the use of cookies and other similar technologies involves processing personal data, this processing is regulated by the 'General Data Protection Regulation (GDPR)'. The UK Data Protection Act 2018 (DPA 2018) also applies, and tailors how the GDPR applies in the UK.[2]

The ePrivacy Directive[3], first passed in the EU in 2002 and amended in 2009 (often referred to as the 'Cookie Directive') remains in force in the UK[4] through The Privacy and Electronic Communications Regulations 2003 (PECR) (referred to as the 'cookie law' – although it does not only apply to cookies). PECR was not replaced or removed by the GDPR.

Note: at some point in the next few years, the ePrivacy Directive is expected to be replaced at EU level with the ePrivacy Regulation. It is not currently clear what this will mean for the UK, in the context of its exit from the EU. However, the proposed ePrivacy Regulation is not currently expected to eliminate the requirement for consent for cookies or the need to manage both ePrivacy and GDPR obligations. Regardless of any future potential changes, companies must continue to comply with the existing law as it currently stands in the UK.

1 PECR have been amended several times since 2003. There is a list of the changes on the ICO's website here.
2 For more details see here.
3 Directive 2002/58/EC 'concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)'.
4 (as well as other EU countries that have implemented it).

Details

PECR sets out the rules surrounding electronic communications and technologies that store information, or gain access to information already stored, on someone's device (whether personal data or not). PECR applies not only to cookies, but to 'related technologies,' including the use of mobile advertising IDs (IDFA, Ad-ID), statistical IDs (fingerprints), and any analogous technology that maintains state on a device or otherwise produces an ID that corresponds to an individual device (deterministically or probabilistically). You should be aware that these technologies may also themselves be considered personal data (and therefore also within the scope of the GDPR). In this guidance, references to 'cookies' should be read as meaning cookies and any other similar technologies that are within the scope of PECR.

PECR does not detail a list of possible legal bases for processing, in the way that the GDPR does. Rather, it requires that all cookies and related technologies have consent prior to activation or use, unless they are 'strictly necessary' to fulfil a user-requested function (or they are used for the sole purpose of carrying out a communication). This requirement applies even if the cookies are not associated with personal data, as defined under the GDPR. The ICO takes a very narrow view of the categories of cookies that qualify as 'strictly necessary' (and therefore do not require prior consent), with many common digital advertising business models failing to meet the test, including advertising, analytics, and measurement cookies (for more details see the ICO's guide to PECR, which contains a section on exemptions).

The requirement for consent under PECR remains in force as a parallel requirement to the GDPR's requirement for a legal basis for processing personal data. In any context that involves access to or storage of information on a device (which in practice is most internet-enabled contexts) companies must find a way to satisfy both of these requirements simultaneously while interacting with consumers.

PECR does not define consent, but refers to the definition of consent in the Data Protection Act (i.e. the definition contained in the GDPR[5]).[6] The GDPR definition of consent is stringent and means that, in practice, you need consent for cookies and other similar technologies, and in order for that consent to be valid, it must meet the requirements for consent specified in the GDPR (see section 3).

You should be aware that, if you need to obtain consent, under the GDPR you are responsible for being able to demonstrate that you have in fact gained valid consent (i.e. in practice, this needs to be recorded in an auditable way). See section 3.

[5] As set out in Article 4 and recital 32 of the GDPR.

[6] ""consent" by a user or subscriber corresponds to the data subject's consent in the GDPR (as defined in section 3(10) of the Data Protection Act 2018)". Regulation 2 of PECR, as amended by Regulation 8 of The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019

Both the requirement to have obtained consent (to GDPR standards), and the requirement to be able to demonstrate this, apply to the entity that is using the cookie. This is the case even if you are relying on another entity (e.g. a publisher or an advertiser) to obtain consent on your behalf.[7]

Other cookie requirements

In addition to requiring consent, PECR also requires that you must tell people if you set cookies, and you must provide clear and comprehensive information (before they give their consent) to explain what the cookies do and why, and who will be using (setting or accessing) them and for what purpose, so that they understand what happens if they allow cookies.

The ICO's cookies guidance says:

> You must explain the way the cookies (or other similar technologies) work and what you use them for, and the explanation must be clear and easily available. Users must be able to understand the potential consequences of allowing the cookies. You may need to make sure the language and level of detail are appropriate for your intended audience.

For more details on the PECR 'information' requirements and guidance on how to comply, see the ICO's cookie guidance.

To comply with PECR, you must meet both the consent and 'information' requirements.

What about legitimate interest?

The legitimate interest legal basis in the GDPR, which is one of the six possible legal bases for processing personal data, is not relevant to the PECR requirements for setting or reading cookies or other information on a device. The consent requirement for cookies is set out in PECR and remains in place alongside the GDPR requirement to establish a legal basis to process personal data. You cannot rely on legitimate interest for the use of any non-essential[8] cookies to store information, or gain access to information already stored, on someone's device.

3. PECR consent under the GDPR

The GDPR sets out a number of conditions that must be met in order for consent to be valid. In addition, under the GDPR, all organisations processing personal data are explicitly

[7] The CJEU ruling on Fashion ID found that in the case of third-party plugins, website operators are joint controllers with plugin data recipients, and therefore both parties are responsible for demonstrating their compliance with joint controller responsibilities under GDPR.

[8] i.e. any cookies or other similar technologies that are not exempt from the consent requirements because they are 'strictly necessary' or are for the sole purpose of carrying out a communication.

responsible for compliance with the Regulation and must be able to demonstrate and evidence this compliance. Therefore, you should ensure that any consent that you obtain is recorded and can be demonstrated if required. The burden of proof is on companies to show that consent has been obtained lawfully, so being able to verify consent is very important, particularly if another organisation obtains consent on your behalf.

Consent is only valid if it is freely given, meaning that people have to be given a free and genuine choice about what you do with their data. This means that consent can be withdrawn at any time and that refusal to consent to data processing cannot be to the user's detriment.

Consent must not be bundled with other terms and conditions. It must be given freely and independently. You cannot ask a consumer to agree to general terms and conditions that includes giving consent to data processing as a sub-condition.

Consent must be informed. The data subject must know your identity and the identity of any joint controllers, and anyone setting third party cookies.

Requests for consent must be clear, unambiguous and easy to action. You cannot use vague language and you cannot pre-tick consent boxes or use other 'default' consent methods (and you therefore cannot set or use any non-essential cookies before consent can be given – see section 4 for more details). Acquiescence is not consent.

Consent must be specific. You must give details of the processing purpose and activities and you, or any processor, must not process the data in question in any other way. The user should be able to freely choose which purposes they do and do not consent to. Consent for cookies, and for each data processing purpose, should be separate from and independent of other purposes (even though in practice, from a business perspective, one purpose may be dependent on another). For example, personalisation of advertising should be separate to analytics.

If you are relying on consent obtained for you by another party you should ensure that this consent meets all the relevant requirements.

Cookie walls

The ICO has indicated that the use of 'cookie walls', whereby access to content or a service is subject to acceptance of (i.e. consent to) non-essential cookies, raises questions about the validity of consent, in terms of whether it is 'freely given'. They recognise, however, that 'there are some differing opinions as well as practical considerations around the use of partial cookie walls'[9] and are continuing to explore this topic further.

9 ICO Blog

Methods of obtaining consent

Approaches that are no longer sufficient to meet the GDPR consent standard under PECR include:

- old-style (i.e. pre-GDPR) cookie banners without detailed and specific information
- navigational consent, whereby a consumer indicates their consent by clicking elsewhere or continuing to use a site
- a consent choice collected without an easy and readily available option to decline consent
- consent collected without a specific mentioning of the individual companies that will benefit from the consent

The ICO's cookie guidance (see section 5 of this document) contains more detail, including a section on how to comply with the cookie rules that covers compliance with both the requirements for consent and the requirement to provide people with clear and comprehensive information about cookies before they give consent.

The Transparency and Consent Framework (TCF)

The cross-industry Transparency and Consent Framework (TCF) was launched in 2018 ahead of GDPR coming into force. The TCF is an industry tool that supports companies within the digital advertising ecosystem as they manage their compliance obligations under the GDPR and ePrivacy Directive.

The TCF's objective is to help all parties in the digital advertising chain ensure that they comply with the EU's GDPR and ePrivacy Directive when processing personal data or accessing and/or storing information on a user's device, such as cookies, advertising identifiers, device identifiers and other tracking technologies. The TCF can be used to manage the transparency and consent requirements of cookies and other similar technologies, including first- and third-party cookies.

The TCF creates an environment where website publishers can tell visitors what data is being collected and how their website and the companies they partner with intend to use it. The TCF gives the publishing and advertising industries a common language with which to communicate consumer consent for the delivery of relevant online advertising and content.

The TCF is comprised of a set of policies and a technical protocol and that have been designed to standardise how companies in the digital advertising industry collect GDPR-standard consent and establish legal bases, while also providing an open source technical spec for storing an auditable status attribute for each consumer and relaying this status to partners and clients where appropriate.

In relation to cookie consent requirements, the TCF specifically includes a 'purpose' related to ePrivacy requirements (described as 'Information storage and access' under version 1.0, and 'Store and/or access information on a device' under version 2.0 – see below) that

facilitates obtaining consent as required by PECR. The TCF enables consent to be 'informed', through provision of the right information to users and 'specific', by providing granular processing purposes that separate 'cookie consent' from consent for other data processing purposes. Within the TCF, where third parties need consent and are relying on first parties to obtain that consent on their behalf, the TCF provides a signal that third parties can use both to know whether they have consent before storing or accessing information on a device, and to be able to demonstrate that consent.

TCF v2.0 was launched in August 2019 and is due to be rolled out from April 2020. It continues to support the overall drive of the TCF to increase consumer transparency and choice, management by digital properties of consent and compliance, and industry collaboration that centres on standardisation.

The TCF is a tool to help support compliance. Companies choosing to use the TCF are responsible for its proper implementation and operation, and for complying with the applicable policies and technical specifications, and remain responsible for their own ePrivacy and GDPR compliance.

For more information about the TCF and version 2.0 see https://www.iabuk.com/policy/tcf-v20-what-you-need-know or contact policy@iabuk.com

4. What this means in practice

Taken together, the consent requirements in PECR and the GDPR mean that you must not set or read cookies or engage in any device level identification unless you have demonstrable, GDPR-style consent (or you meet the narrow 'strictly necessary' exception), and you have met the requirement to provide users with clear information about the cookies you intend to use.

Until consent is obtained, cookies must not be set and tracking at the device level cannot be initiated.

What this means for media properties

If you operate a site or mobile property serving the UK you should ensure that you have conducted an analysis of the cookies and other tracking technologies currently integrated into your sites/apps, including the related data processing activities. The ICO's cookie guidance contains a section on how to conduct a cookie audit.

You must ensure that you have consent for both your own use of cookies, and that you also assist in the establishment of consent for your third-party partners, both direct and indirect.

Many media properties are partnering with Consent Management Platforms (CMPs), a new class of company providing consent platforms to assist with the establishment of consent on

your properties (as well as other legal bases). CMPs are a key component part of the TCF (see section 3, above). For more information see https://iabeurope.eu/tcf-for-publishers/.

What this means for third party technology/intermediary companies

Third parties typically use their own technologies (including cookies) to identify an individual device, and therefore usually need to establish consent under PECR regardless of whether or not they are controllers or processors, and regardless of their legal basis under the GDPR.

The TCF is designed specifically to help third parties to establish consent and participation is highly recommended. Third party technology/intermediary companies can register as a 'vendor' and utilise the TCF to establish valid GDPR-style consent, as required under PECR. For more information see https://iabeurope.eu/tcf-for-vendors/.

What this means for advertisers

If you own or operate media properties (sites/apps), refer to the relevant advice above. Advertisers should use the TCF to manage PECR consent for cookies, etc. on their media properties wherever practical. For example, advertisers can use a TCF CMP to establish PECR consent and a legal basis for themselves (via non-TCF first party consent) and their advertising partners (for example, retargeting partners) as vendors in the TCF. This approach will provide for the advertiser's direct compliance on their own properties, while also enabling their key marketing partners to act on their behalf.

For more information see https://iabeurope.eu/tcf-for-advertisers-agencies/ and https://iabeurope.eu/tcf-for-publishers/.

5. Further reading and resources

Legislation

- The Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR). Regulation 6 covers cookies. (n.b. PECR transposes the ePrivacy Directive into UK law).
- Data Protection Act 2018

ICO guidance

- Guide to PECR – Cookies and similar technologies
- Guidance on the use of cookies and similar technologies
- ICO 'myth-busting' cookies blog: 'What does good look like?'
- Guidance on GDPR and consent
- Data protection and Brexit

Case law examples relating to cookies and consent (note: these are not UK-based examples)

- The Court of Justice of the European Union (CJEU) found that (i) use of pre-ticked boxes for cookie consent is unlawful, (ii) any consent obtained regarding cookies cannot be sufficiently informed in compliance with applicable law if the user cannot reasonably comprehend how the cookies employed on a given website will function. The CJEU applied the GDPR definition of consent
- PwC was fined €150,000 for applying consent inappropriately
- Vueling was fined €30,000 for having no effective way of consenting to cookies
- The Belgian regulator fined a small law firm €15,000 for non-compliant cookie practices. This is especially of note since no complaint was made and the business complied with the regulator's instructions for rectification