Privacy and Electronic Communications Regulations

Guidance on the use of cookies and similar technologies

ico.
Information Commissioner's Office

About this guidance

The Privacy and Electronic Communications Regulations (PECR) cover the use of cookies and similar technologies for storing information, and accessing information stored, on a user's equipment such as a computer or mobile device.

This guidance addresses cookies and similar technologies in detail. Read it if you operate an online service, such as a website or a mobile app, and need a deeper understanding of how PECR applies to your use of cookies.

If you haven't yet read the Cookies page in the Guide to PECR, you should read that first. It sets out the key points you need to know.

Contents

- How does cookie consent fit with the lawful basis requirements of the GDPR?
- Do the rules apply to the processing of personal data gained via cookies?
- What about the proposed ePrivacy Regulation?

How do we comply with the cookie rules?

- Who is responsible for compliance?
- How do we plan and decide what type of cookies will be used?
- How should we conduct a cookie audit?
- How do we tell people about cookies?
- What if children are likely to access our online service?
- How should we request consent in practice?
- Can we use message boxes and similar techniques
- Can we rely on settings-led consent?
- Can we rely on feature-led consent?
- Can we rely on browser settings and other control mechanisms?
- Can we use 'terms and conditions' to gain consent for cookies?
- Can we use 'cookie walls'?
- Can we pre-enable any non-essential cookies?
- What if we use third-party cookies?
- Are analytics cookies exempt?
- How do the exemptions apply to different types of cookies?
- What if our users change their minds about cookies?
- How often should we get consent?
- How should we keep records of user preferences?
- How long should our cookies last?

What else do we need to consider?

- What if our use of cookies changes?
- What about cookies set on websites that we link to?
- What about cookies set on overseas websites?
- Can public authorities set cookies on their websites?
- What about other devices like mobiles, smart TVs, wearables, and the 'Internet of Things'?
- What happens if we don't comply?

What are cookies and similar technologies?

In detail

What are ‘cookies’?

Cookies are small pieces of information, normally consisting of just letters and numbers, which online services provide when users visit them. Software on the user's device (for example a web browser) can store cookies and send them back to the website next time they visit.

How are cookies used?

Cookies are a specific technology that store information between website visits. They are used in numerous ways, such as:

- remembering what’s in a shopping basket when shopping for goods online;
- supporting users to log in to a website;
- analysing traffic to a website; or
- tracking users' browsing behaviour.

Cookies can be useful because they allow a website to recognise a user’s device. They are widely used in order to make websites work, or work more efficiently, as well as to provide information to the owners of the site. Without cookies, or some other similar method, websites would have no way to ‘remember’ anything about visitors, such as how many items are in a shopping basket or whether they are logged in.

What are ‘session’ and ‘persistent’ cookies?

Cookies that expire at the end of a browser session (normally when a user exits their browser) are called ‘session cookies’. Cookies that can be stored for longer are called ‘persistent cookies’. PECR applies to both types.

Session cookies allow websites to recognise and link the actions of a user during a browsing session. They may be used for a variety of purposes such as remembering what a user has put in their shopping basket as they browse around a site.

Cookies can also be used for security purposes, such as when a user logs in to internet banking or their webmail. These session cookies expire after a session ends, so would not be stored beyond this. For this reason session cookies may sometimes be considered less privacy-intrusive than persistent cookies.

Persistent cookies are stored on a user’s device in-between sessions. They can allow the preferences or actions of the user across a site (or across different websites) to be remembered.

Persistent cookies may be used for a variety of purposes including remembering users’ preferences and choices when using a site or to target advertising. The length of time between a cookie being set and expiry is set by the website operator. A user can also delete previously set persistent cookies manually or configure the browser settings to delete cookies at a set interval.

What are ‘first-party’ and ‘third-party’ cookies?

Whether a cookie is ‘first’ or ‘third’ party refers to the website or domain placing the cookie.

First-party cookies are set directly by the website the user is visiting, ie 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. This typically occurs when the website incorporates elements from other sites, such as images, social media plugins or advertising. When the browser or other software fetches these elements from the other sites, they can set cookies as well.

What are ‘similar technologies’?

Functions usually performed by a cookie can be achieved by other means. This could include, for example, using certain characteristics to identify devices so that visits to a website can be analysed.

PECR applies to any technology that stores or accesses information on the user’s device. This could include, for example, HTML5 local storage, Local Shared Objects and fingerprinting techniques.

Example

Device fingerprinting is a technique that involves combining a set of information elements in order to uniquely identify a particular device.

Examples of the information elements that device fingerprinting can single out, link, or infer include (but are not limited to):

- data derived from the configuration of a device;
- data exposed by the use of particular network protocols;
- CSS information;
- JavaScript objects;
- HTTP header information,
- clock information;
- TCP stack variation;
- installed fonts;
- installed plugins within the browser; and
- use of any APIs (internal and/or external).

It is also possible to combine these elements with other information, such as IP addresses or unique identifiers, etc.

PECR also applies to technologies like scripts, tracking pixels and plugins, wherever these are used.

Example

An organisation conducts electronic marketing and incorporates a tracking pixel within the emails. The pixels record information including the time, location and operating system of the device used to read the email.

Whilst the majority of electronic mail marketing is governed by Regulation 22 of PECR, where tracking pixels store information, or gain access to information stored, on a user's device Regulation 6 also applies.

PECR does not prohibit using cookies and similar technologies. However, PECR does require you to tell people about them and give them the choice as to whether or not this information is stored on their devices in this way.

From now on, this guidance uses the single term 'cookies' to refer to cookies and similar technologies that PECR applies to, including when used in other contexts such as a mobile app.

What are the rules on cookies and similar technologies?

In detail

What does PECR say about cookies and similar technologies?

PECR does not refer to cookies by name, but Regulation 6 states:

> (1) … a person shall not store or gain access to information stored, in the terminal equipment of a subscriber or user unless the requirements of paragraph (2) are met.
>
> (2) The requirements are that the subscriber or user of that terminal equipment —
>
> (a) is provided with clear and comprehensive information about the purposes of the storage of, or access to, that information; and
>
> (b) has given his or her consent.

This means that if you use cookies you must:

- say what cookies will be set;
- explain what the cookies will do; and
- obtain consent to store cookies on devices.

PECR also applies to 'similar technologies' like fingerprinting techniques. Therefore, unless an exemption applies, any use of device fingerprinting requires the provision of clear and comprehensive information

as well as the consent of the user or subscriber.

Further Reading

> Relevant provisions in PECR - See Regulation 6 of the 2003 version of PECR
> External link

> Relevant provisions in PECR - See the amendment made in 2011.
> External link

Who are 'subscribers' and 'users'?

The cookie rules apply to the 'terminal equipment' of the 'subscriber or user'. The 'subscriber' means the person who pays the bill for the use of the line. The 'user' is the person using the computer or other device to access an online service.

In many cases the subscriber and the user may be the same, for example when an individual uses their broadband connection to access a website on their computer or mobile device – that person would be the 'user' as well as the 'subscriber' if they pay for the connection.

However, this is not always the case. For example, if a family member visits that subscriber's home and uses the internet connection to access your service from their own device, they would be the user.

What is 'terminal equipment'?

This refers to the device a cookie is placed on – typically a computer or mobile device, but also other equipment such as wearable technology, smart TVs, and connected devices including the 'Internet of Things'.

What does 'clear and comprehensive information' mean?

PECR does not define what 'clear and comprehensive information' means. However, Article 5(3) of the ePrivacy Directive says that clear and comprehensive information should be provided 'in accordance with' data protection law.

This relates to the UK GDPR's transparency requirements and the right to be informed. It means that when you set cookies you must provide the same kind of information to users and subscribers as you would do when processing their personal data (and, in some cases, your use of cookies will involve the processing of personal data anyway).

The information has to cover:

- the cookies you intend to use;
- the purposes for which you intend to use them;
- any third parties who may also process information stored in or accessed from the user's device; and
- the duration of any cookies you wish to set.

These requirements also apply to cookies set by any third parties whose technologies your online service incorporates – this would include cookies, pixels and web beacons, JavaScript and any other

means of storing or accessing information on the device including those from other services such as online advertising networks or social media platforms.

The recitals of the ePrivacy Directive further clarify that:

- 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.

Whilst providing information about cookies equates to the transparency requirements of data protection law, levels of user understanding will differ. If you use cookies you will need to make a particular effort to explain their activities in a way that all people will understand.

Long tables or detailed lists of all the cookies operating on the site may be the type of information that your users will want to consider. Some sites might use tens or even hundreds of cookies and therefore it may also be helpful to provide a broader explanation of the way cookies operate and the categories of cookies in use. For example, a description of the types of things you use analytics cookies for on the site will be more likely to satisfy the requirements than simply listing all the cookies you use with basic references to their function.

Further Reading

Relevant provisions in the ePrivacy Directive See Article 5(3) and Recital 66 of the 2009 amendment to the ePrivacy Directive
External link

Relevant provisions in the ePrivacy Directive - See Recital 25
External link

Relevant provisions in the UK GDPR - See Articles 12 to 14 and Recitals 58 and 60-62
External link

Further reading – ICO guidance

The right to be informed

What does ‘consent’ mean?

PECR requires that users or subscribers consent to cookies being placed or used on their device. There is no definition of consent given in PECR or in the ePrivacy Directive; instead, the UK GDPR definition of consent applies. This is in Article 4(11) of the UK GDPR and states:

> "'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."

Regulation 8(2) of the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019 clarifies that, for PECR:

> "'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)."

Article 7 of the UK GDPR provides further specifics about consent requirements, saying that:

- you must be able to demonstrate that you have valid consent;
- your consent requests must be 'clearly distinguishable from other matters' – ie, they must not be bundled as part of terms and conditions;
- 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.

Recital 32 of the UK GDPR also specifically bans pre-ticked boxes – silence or inactivity does not constitute consent.

In respect of 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).

Further Reading

Relevant provisions in the UK GDPR - See Articles 4(11) and 7, and Recitals 32, 42 and 43.
External link

Relevant provisions in the Data Protection, Privacy and Electronic Communications (Amendments etc.) (EU Exit) Regulations 2019 - See Regulation 8(2)
External link

Further reading – ICO guidance

Consent

Further reading – European Data Protection Board

The European Data Protection Board (EDPB), which has replaced the Article 29 Working Party (WP29), includes representatives from the data protection authorities of each EU member state. It adopts guidelines for complying with the requirements of the EU version of the GDPR.

The EDPB has published Guidelines 05/2020 on consent.

While these guidelines are no longer directly relevant to the UK regime and are not binding under the UK regime, they may still provide helpful guidance.

Who do we need consent from?

PECR states that consent for a cookie should be obtained from the subscriber or user.

In practice, you may not be able to distinguish between consent provided by the subscriber or the user. The key issue is that one of the parties must provide valid consent.

PECR does not specify whether the user or subscriber's wishes should take precedence if individuals have different preferences in respect of the setting of cookies. Other references in PECR to a subscriber's ability to make decisions in this area, such as around browser settings, might suggest the subscriber's preferences take priority, although in some circumstances this will not always be the case.

Example

An employer (the subscriber) provides an employee (the user) with a device at work, along with access to certain services to carry out a particular task. Completing the task effectively depends on using a service that uses cookies, and a device that accepts them.

In this case it is reasonable for the employer's wishes to take precedence.

There are other sections of PECR, concerning browser settings, where the subscriber clearly has the ability to make a decision on behalf of any user. However, there will also be circumstances where a user's wishes should take precedence.

In a domestic context there will usually be one subscriber (the person in the household paying the bill) and potentially several other users. If a user complained that your website was setting cookies without their consent you could demonstrate compliance with PECR if you could show that consent had previously been obtained from the subscriber.

In practice, the key to resolving problems is to ensure information about cookies and mechanisms for making choices are as easily accessible as possible to all users.

Are we required to provide information and obtain consent for all cookies?

No – PECR has two exemptions to the cookie rules. Regulation 6(4) states that:

> (4) Paragraph (1) shall not apply to the technical storage of, or access to, information -
>
> (a) for the sole purpose of carrying out the transmission of a communication over an electronic communications network; or
>
> (b) where such storage or access is strictly necessary for the provision of an information society service requested by the subscriber or user.

These are known as the 'communication' exemption and the 'strictly necessary' exemption.

Further Reading

Relevant provisions in PECR - See Regulation 6 of the 2003 version of PECR
External link

Relevant provisions in PECR - see the amendment made in 2011
External link

What is the 'communication' 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, three elements are considered necessary:

- the ability to route information over a network, by identifying the communication 'endpoints' – devices that accept communications across that network;
- the ability to exchange data items in their intended order; and
- the ability to detect transmission errors or data loss.

The communication exemption therefore includes cookies that fulfil one (or more) of these properties, but only for the sole purpose of the transmission.

So, for the exemption to apply, the transmission of the communication must be impossible without the use of the cookie. Simply using a cookie to assist the communication is insufficient for the exemption to

apply.

What is the ‘strictly necessary’ exemption?

This exemption applies for ‘information society services’ (ISS) – ie, a service delivered over the internet, such as a website or an app. If you are running an online service it is likely that you are operating an ISS.

The ‘strictly necessary’ exemption means that storage of (or access to) information should be essential, rather than reasonably necessary. It is also restricted to what is essential to provide the service requested by the user. It does not cover what might be essential for any other uses that you might wish to make of that data. It is therefore clear that the strictly necessary exemption has a narrow application.

‘Strictly necessary’ also includes what is required to comply with any other legislation that applies to you, for example, the security requirements of data protection law.

Where the setting of a cookie is deemed ‘important’ rather than ‘strictly necessary’, you are still obliged to provide information about the storage or access to the user or subscriber and obtain consent.

Example

A user visits an e-commerce website and decides to purchase a product. They add it to their shopping basket before continuing browsing for more goods they wish to buy. They then finish their shopping by going through the website’s checkout process.

The website uses cookies to ensure that when the user chooses the goods they wish to buy and clicks the ‘add to basket’ or ‘proceed to checkout’ button, the site ‘remembers’ what they chose on a previous page.

In this context, the cookie is ‘strictly necessary’ to provide the service the user requests and so the exemption would apply and no consent would be required.

Although the exemption applies to both the provision of information and the gaining of consent, it is good practice to continue to provide clear information about all cookies including those that are strictly necessary, and if personal data is involved then you will be required to do this under the fairness and transparency requirements of data protection law.

It is important to remember that what is ‘strictly necessary’ should be assessed from the point of view of the user or subscriber, not your own. So, for example whilst you might regard advertising cookies as ‘strictly necessary’ because they bring in revenue that funds your service, they are not ‘strictly necessary’ from the user or subscriber’s perspective.

What activities are likely to meet the ‘strictly necessary’ exemption?

Activities likely to fall within the ‘strictly necessary’ exemption include those that relate to the specific functionality of your service – ie, without them, the user would be unable to undertake certain activities. Cookies that don’t relate to what is strictly necessary would need consent.

Common examples include:

Activity	Likely to meet the 'strictly necessary' exemption?
A cookie used to remember the goods a user wishes to buy when they go to the checkout or add goods to their shopping basket;	✓
Cookies that are essential to comply with the UK GDPR's security principle for an activity the user has requested – for example in connection with online banking services	✓
Cookies that help ensure that the content of a page loads quickly and effectively by distributing the workload across numerous computers (this is often referred to as 'load balancing' or 'reverse proxying')	✓
Cookies used for analytics purposes, eg to count the number of unique visits to a website	**x**
First and third-party advertising cookies (including those used for operational purposes related to third-party advertising, such as click fraud detection, research, product improvement, etc.)	**x**
Cookies used to recognise a user when they return to a website so that the greeting they receive can be tailored	**x**

Also, if you say a cookie is strictly necessary because it fulfils a purpose, such as security, you must ensure that your use is only for that purpose. If you use any information for secondary purposes, the cookie would not be regarded as strictly necessary and you would then need consent.

For more information about how the exemptions work for different types of cookies, read the section 'How do we comply with the cookie rules'.

Further reading – European Data Protection Board

The European Data Protection Board (EDPB), which has replaced the Article 29 Working Party (WP29), includes representatives from the data protection authorities of each EU member state. It adopts guidelines for complying with the requirements of the EU version of the GDPR.

For more information about the types of cookies and how they align with the two exemptions, read the Article 29 Working Party's 'Opinion 04/2012 on cookie consent exemption' and 'Opinion 09/2014 on device fingerprinting'.

You should note that while these guidelines are no longer directly relevant to the UK regime, they may still provide helpful guidance, particularly as their content relates to the cookie rules in PECR.

Do the rules only apply to websites?

No. The use of cookies and similar technologies is not limited to traditional websites and web browsers. The rules in PECR apply to any technique that stores information, or accesses information stored, in the terminal equipment of the subscriber or user.

For example, mobile apps commonly communicate with websites and web services which can set cookies and PECR also covers these. Mobile apps may also be developed with embedded SDKs or other frameworks. These can store information, or access information stored, on the device for various purposes.

Ultimately, whether you run a website, a mobile app, or any other kind of service, you are responsible for understanding the behaviour of any software components that may store information, or access information stored, in a user's device. This is particularly important where you are incorporating someone else's software component, eg third party code.

Do the rules apply to our internal network?

The rules do not apply in the same way to intranets. An intranet is unlikely to be a public electronic communications service, and therefore PECR would not apply in the same way to cookies that are set on an intranet. However, it is important to remember that the requirements of data protection law are still likely to apply if the usage of cookies is for the purposes of monitoring performance at work, for example.

Wherever you collect personal data using cookies then the requirements of data protection law will also apply.

How do the cookie rules relate to the GDPR?

In detail

What is the relationship between PECR and the UK GDPR?

PECR sits alongside the Data Protection Act 2018 (DPA) and the UK GDPR, and provides specific rules in relation to privacy and electronic communications. Where these rules apply, they take precedence over the DPA and the UK GDPR. This is important, because if you are setting cookies you need to consider PECR compliance first **before** you look to the UK GDPR.

Additionally, PECR depends on data protection law for some of its definitions. For example, as the previous section states, PECR takes the UK GDPR's standard of consent. The UK GDPR also talks about cookies within the definition of personal data.

Essentially, if you are operating an online service, then the easiest way to look at the two laws is:

- if your online service stores information, or accesses information stored, on user devices then you should ensure that comply with PECR first, including the requirements to provide information and obtain consent; and
- the UK GDPR applies to any processing of personal data outside of this storage or access.

Regulation 4 of PECR is also clear about the relationship with data protection law:

> 'Nothing in these Regulations shall relieve a person of his obligations under the data protection legislation in relation to the processing of personal data.'

Although PECR does not just apply where personal data is being processed, activities involving the processing of personal data generally have greater privacy and security implications.

Where the setting of a cookie does involve the processing of personal data, you will also need to make sure you comply with the additional requirements of the UK GDPR.

Further Reading

Relevant provisions in PECR - see Regulation 4
External link

Relevant provisions in PECR - see the amendment made to it by Schedule 19 of the Data Protection Act 2018
External link

What does the UK GDPR say about cookies?

The UK GDPR classes cookie identifiers as a type of 'online identifier', meaning that in certain circumstances these will be personal data. For example, a user authentication cookie would involve processing of personal data, as it is used to enable the user to log in to their account at an online service.

Article 4(1) of the UK GDPR defines personal data as:

> 'any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person'

Recital 30 provides further information on the term 'online identifier':

> "Natural persons may be associated with online identifiers provided by their devices, applications, tools and protocols, such as internet protocol addresses, cookie identifiers or other identifiers such as radio frequency identification tags. This may leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them."

It is important to note that cookies may not always be classed as personal data. However, PECR applies whether or not the storage of or access to information on user devices involves processing personal data.

'Online identifiers' can also include (but are not limited to) things like:

- MAC addresses;
- advertising IDs;
- pixel tags;
- account handles; and
- device fingerprints.

The use of these could leave traces which, when combined with unique identifiers and other information, could be used to create profiles of individuals and identify them.

When assessing if an individual is identifiable, you must consider whether online identifiers, on their own or in combination with other information that may be available to those processing the data, may be used to distinguish one user from another.

For example, this is likely to be the case where identifiers are used or combined to create profiles of individuals, even when those individuals are unnamed. This may be either as a named individual or simply as a unique user of electronic communications and other internet services who may be distinguished from other users.

You should be aware that that whilst a single information element may not be personal data on its own, the combination of multiple elements makes it more likely that the information will constitute personal data. This is particularly the case when the information enables you to single out, make inferences or take specific actions in relation to users (such as identifying them over time or across multiple devices and websites, even if you don't know the name of those users). Where this is the case, your processing must comply with the UK GDPR.

When considering alternatives to cookies it is also important to look at the broader privacy context. Even where the cookie rules do not apply, you may need to comply with the GDPR. For example, if information is collected that builds up a picture allowing an individual to be identified, those individuals need to be told what information is being collected, as well as how and why.

Further reading – ICO guidance

'What is personal data?'

The right to be informed

Further reading – European Data Protection Board

The European Data Protection Board (EDPB), which has replaced the Article 29 Working Party (WP29), includes representatives from the data protection authorities of each EU member state. It adopts guidelines for complying with the of the EU version of the GDPR.

In 2014, WP29 produced guidance on device fingerprinting and the ePrivacy Directive in Opinion 9/2014. This provides more information about how PECR applies in this context, and also outlines the data protection risks related to device fingerprinting. This guidance remains applicable as it relates to the ePrivacy Directive.

How does cookie consent fit with the lawful basis requirements of the UK GDPR?

To process personal data, you must have a lawful basis. The UK GDPR has six lawful bases, of which one is consent. No lawful basis is more important than the other – the appropriate one depends on the specifics of your processing.

However, PECR requirements are separate from, and different to, those of the UK GDPR. Guidance produced by European data protection authorities on how the ePrivacy Directive relates to the UK GDPR clarifies that, if consent is required under the cookie rules:

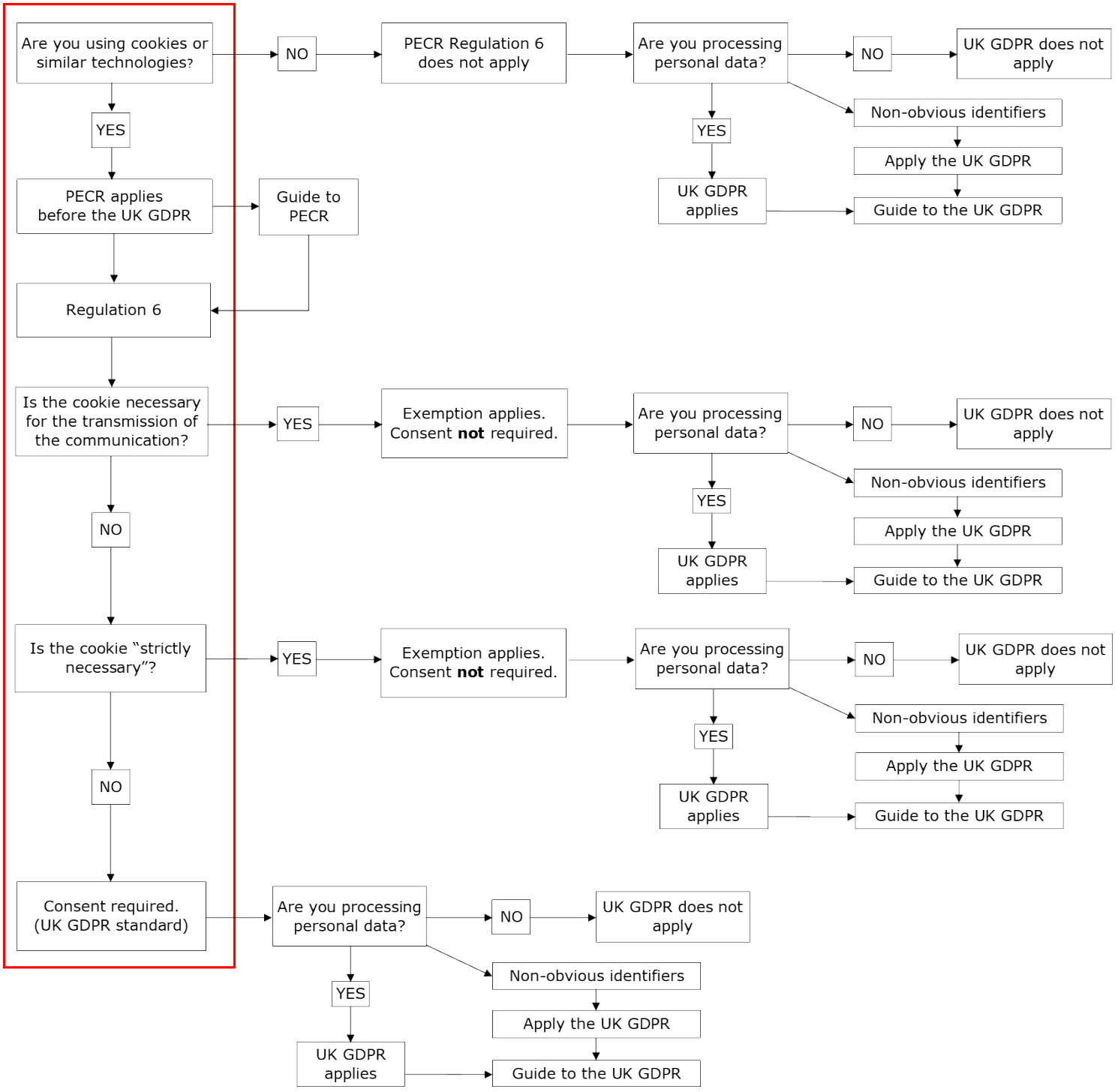
> "the controller cannot rely on the full range of possible lawful grounds provided by article 6 of the UK GDPR".

The simplest way to understand it is that if your cookies require consent under PECR, then you cannot use one of the alternative lawful bases from the GDPR to set them. If you're setting cookies, this is why you need to look to PECR first and comply with its specific rules, before considering any of the general rules in the UK GDPR.

If the cookies you set aren't exempt from Regulation 6, then you can only use consent – and this must be of the UK GDPR standard. This is also the case whether or not personal data is involved. If you have obtained consent in compliance with PECR, then in practice consent is also the most appropriate lawful basis under the UK GDPR. Trying to apply another lawful basis such as legitimate interests when you already have UK GDPR-compliant consent would be an entirely unnecessary exercise, and would cause confusion for your users.

If your cookie meets one of the exemptions, then the requirement to have consent to set it doesn't apply – essentially, the technical process of storing or accessing information on the device falls out of PECR and, where personal data is involved, the UK GDPR then applies.

Figure 1 below demonstrates where consent applies for cookies.



Use our tool to determine where consent applies for your use of cookies.

Further reading – European Data Protection Board

The European Data Protection Board (EDPB), which has replaced the Article 29 Working Party (WP29), includes representatives from the data protection authorities of each EU member state. It adopts guidelines for complying with the requirements of the EU version of the GDPR.

The EDPB has published 'Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR'.

While this Opinion is no longer directly relevant to the UK regime and is not binding under the UK

regime, it may still provide helpful guidance about how the cookie rules relate to the EU GDPR.

Do the rules apply to the processing of personal data gained via cookies?

PECR has rules for the storing of information, or accessing information stored, on user devices. It does not contain any specific rule for prior or subsequent processing operations involving this information.

So, where personal data is involved, it may be possible to rely on an alternative lawful basis for subsequent processing beyond the setting of any cookies. However, you, will need to consider the specifics very carefully, particularly if the envisaged processing includes sharing that data with third parties.

You should also be aware that European data protection authorities, including the ICO, have previously stated that, in certain cases the processing of personal data that follows (or depends on) the setting of cookies is highly likely to require consent as its lawful basis.

This is not just because the personal data originates by the use of cookies (and therefore consent is required under PECR) but is also because of the nature, scope, context and purpose(s) of the processing operations themselves mean that users must be informed, and agree, to the processing prior to it taking place in order to ensure that it is fair.

Analysing or predicting preferences or behaviour

Where personal data obtained via the use of cookies and similar technologies is used for purposes such as analysing or predicting the personal preferences, behaviour and attitudes of individuals, with this subsequently informing measures or decisions taken about them consent is likely to be required otherwise this further use cannot be considered compatible.

Example

Tracking and profiling for direct marketing and advertising

For similar reasons, consent would be required for processing like tracking and profiling for purposes of direct marketing, behavioural advertisement, data-brokering, location-based advertising or tracking-based digital market research due to the nature of the processing operations and the risks posed to individuals.

The fact that consent is also required under PECR means that in most circumstances, legitimate interests is not considered to be an appropriate lawful basis for the processing of personal data in connection with profiling and targeted advertising.

Consent will be required under PECR for the use of cookies in these circumstances, and in practice, consent is therefore the most applicable lawful basis for any subsequent processing of personal data for the purposes described.

Further reading - European Data Protection Board

The European Data Protection Board (EDPB), which has replaced the Article 29 Working Party (WP29), includes representatives from the data protection authorities of each EU member state. It adopts guidelines for complying with the requirements of the EU version of the GDPR.

The EDPB has published 'Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR'. This provides useful information about how the cookie rules relate to the EU GDPR and re-states the positions previously taken by WP29 about when consent should be required for certain processing operations beyond the setting of cookies.

WP29 previously published 'Opinion 3/2013 on purpose limitation' and 'Opinion 6/2014 on the notion of legitimate interests'. Although this guidance was produced under the previous data protection framework, much of it applies under the EU GDPR.

While these Opinions are no longer directly relevant to the UK regime and are not binding under the UK regime, they still provide helpful guidance on these issues.

What about the proposed ePrivacy Regulation?

The ePrivacy Regulation (ePR) is a piece of European legislation that is currently under development. When finalised, it will replace the ePrivacy Directive on which PECR is based. It intends to provide updated and modernised rules for privacy and electronic communications.

However, we cannot provide any specific guidance on what the ePR may contain in the future.

You should however note that irrespective of the development of the ePR, PECR continues to apply in full, alongside the UK GDPR.

How do we comply with the cookie rules?

In detail

Who is responsible for compliance?

PECR says that 'a person' shall not store, or gain access to information stored, on user devices. However, PECR does not define who should be responsible for complying with the requirement to provide information about cookies and obtain consent. The key point is not who obtains the consent but that you provide clear and comprehensive information and obtain valid consent.

Where you operate an online service and any use of cookies will be for your own purposes, it is clear that you will be responsible. The person setting the cookie is therefore primarily responsible for compliance with the requirements of PECR, although this is not necessarily the case where multiple parties are involved.

How do we plan and decide what type of cookies to use?

If you are planning a new online service, you should take steps to detail what cookies you will use, which are strictly necessary, and ensure that you have appropriate arrangements in place with any third

parties.

For any pre-existing services, you should already know what types of cookies you use but it would be sensible to recheck. This might take the form of a comprehensive 'cookie audit' of your online service, or it could be as simple as checking what data will be sent to users and why.

How should we conduct a cookie audit?

When you conduct a cookie audit, you should:

- for cookies that are already present, identify those that are operating on or through your website, using a combination of browser-based tools and server-side code review;
- confirm the purpose(s) of each of the cookies you use (or intend to use);
- confirm whether cookies are linked to other information held about users – such as usernames – and whether your use of cookies also involves (or will involve) processing personal data;
- identify what data each cookie holds or otherwise processes;
- confirm the type of cookie – session or persistent;
- distinguish between which cookies are strictly necessary and which ones aren't (and would therefore require clear and comprehensive information and consent);
- ensure that your consent mechanism enables users to control the setting of all non-essential cookies;
- determine the lifespans of any persistent cookies and whether these durations are justifiable for the stated purpose;
- determine whether each cookie is a first or third party cookie, and if it is a third party cookie who is setting it;
- double check that the privacy information provides accurate and clear information about each cookie;
- confirm what information you share with third parties, and what users are told about this; and
- document your findings and follow-up actions, and build in an appropriate review period.

If your service already uses cookies, you should look at this as opportunity to 'clean up' existing web pages and stop using cookies that are unnecessary or which have been superseded as your site has evolved.

Don't just do this once. Your usage of any third party content is likely to change over time, so it is good practice to undertake regular reviews of your cookie usage, as well as any third party services your website includes that may set cookies.

Once you have completed the audit, the next consideration is the best methods for providing information and requesting consent.

How do we tell people about cookies?

To comply with the information requirements of PECR, you need to make sure users will see clear information about cookies. In any case, doing so will increase levels of user awareness and control, and also assist in gaining valid consent.

You also need to tell people about 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. This 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.

You should consider how the design of your online service impacts on the visibility of the link to your policy. For example, a link at the bottom of a concise webpage which has no content "below the fold" will be much more visible and accessible than a link in the footer of a dense webpage of 10,000 words. In this case a link in the header would be more appropriate.

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 ("Find out more about how our site works and how we put you in control.")

You also need to ensure the information is clear so that your users understand it. Consider tailoring the language to your audience, and not using lengthy and overly complex terminology.

What if children are likely to access our online service?

The rules are no different if children access your online service. You will need to provide clear and comprehensive information about your use of cookies and ensure you have consent for any that are not strictly necessary.

However, if children are likely to access your service you will need to ensure that both the information you provide and the consent mechanism you use are appropriate for children.

More generally, if your online service is likely to be accessed by a child then you will also need to comply with the requirements of the ICO's code of practice on age appropriate design.

Further reading – ICO guidance

The Children's Code hub

Key data protection themes - Children

How should we request consent in practice?

How you request consent for cookies will depend initially on what the cookies in use are doing and, to some extent, on the relationship you have with your users.

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.

You may also find it helpful to look at the methods other online services already use.

You need to ensure that any consent mechanism you put in place allows users to have control over all the cookies your website sets, not just your own.

For example, if you want to set third-party content such as tracking pixels and beacons from social networks, you need to ensure that users are given information about these and appropriate controls to signify whether or not they consent.

In practice, this can be challenging as not all consent mechanisms presently enable users to disable cookies from third parties directly. However, designing and implementing a consent mechanism that works only for some of the cookies would not be compliant with PECR, as the user is not provided with any control over these cookies – they must visit different websites and take different actions to disable them.

Ultimately, you are the one who determines what cookies are set on your website, and in particular the number and type of third-party cookies involved. One of the considerations before incorporating a third-party cookie should therefore be whether your consent mechanism allows the user to control whether the cookie is set or not.

Can we use message boxes and similar techniques?

Message boxes such as banners, pop-ups, message bars, header bars or similar techniques might initially seem an easy option for you to achieve compliance.

However, you need to consider their implementation carefully, particularly in respect of the implications for the user experience. For example, 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. Similarly, long lists of checkboxes might seem like a way to make your consent mechanism appropriately granular, but this approach carries different risks in that your users may simply not interact with the mechanism or may not understand the information you're providing.

At the same time, Recital 32 of the UK GDPR is clear that electronic consent requests must not be unnecessarily disruptive – so you need to consider how you go about providing clear and comprehensive information without confusing users or disrupting their experience. However, this does not override the need to ensure that consent requests are valid – so some level of disruption may be necessary.

Consent can still be sought in this way provided it makes the position absolutely clear to users. Many websites routinely use pop-ups or 'splash pages' to make users aware of changes to the site or to ask for their feedback. Similar techniques could be a useful way of highlighting the use of cookies and consent.

There are challenges with using these techniques. If users do not click on any the options available and go straight through to another part of your site, and you go ahead and set non-essential cookies on their devices, this would not be valid consent. This is because users who fail to engage with the consent box cannot be said to consent to the setting of these cookies.

Can we rely on settings-led consent?

Some cookies are deployed when a user makes a choice over a site's settings. In these cases, consent

could be sought as part of the process by which the user confirms what they want to do, or how they want the site to work.

For example, some websites 'remember' which version a user wants to access, such as a version of a site in a particular language, or what font size to use. These cookies are sometimes known as 'preference cookies' or 'user interface' 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. It might be the size of the text they want to have displayed, the colour scheme they like or even the 'personalised greeting' they see each time they visit the site.

You must however take care 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 we rely on feature-led consent?

Your site could include video clips or remember what users have done on previous visits in order to personalise the content they are service. Some cookies would then be stored if the user chooses a particular feature of your site.

However, you still need to provide clear and comprehensive information and obtain consent.

Where the feature is provided by a third party, users will need to be made aware of this, and be given information on how the third party uses cookies and similar technologies so that the user is able to make an informed choice.

Further reading – ICO guidance

Consent

Further reading – European Data Protection Board

The European Data Protection Board (EDPB), which has replaced the Article 29 Working Party (WP29), includes representatives from the data protection authorities of each EU member state. It adopts guidelines for complying with the requirements of the EU version of the GDPR.

The EDPB has published Guidelines 05/2020 on consent.

While these guidelines are no longer directly relevant to the UK regime and are not binding under the UK regime, they may still provide helpful guidance.

Can we rely on browser settings and other control mechanisms?

You cannot assume that each visitor to your online service can configure their browser settings to correctly reflect their preferences in relation to the setting of cookies.

PECR suggests that 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. Regulation 6(3)(a) states:

> ‘consent may be signified by a subscriber who amends or sets controls on the internet browser which the subscriber uses or by using another application or program to signify consent.’

This is where the user or subscriber sets up their browser so that only certain cookies are allowed.

Example

A user visits a website that can identify that their browser is set up to allow cookies of types A, B and C but not of type D.

As a result the website owner can be confident that in setting cookies A, B and C they have the user’s consent to do so. They would not set cookie D.

For consent to be clearly signified it would need to be clear that users and subscribers had been prompted to consider their current browser settings. This would require evidence of either a positive action that the subscriber was happy with the default, or otherwise made a decision to change the settings.

Browsers may also include other features such as tracking protection options. Depending on the browser, these may be either enabled by default or require the user to configure them. There is also a range of browser extensions and add-ons for various web browsers that users can install to further manage their cookie preferences.

However, you should be aware 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. This is particularly important when considering web browsers and apps on other devices such as smartphones, tablets, smart TVs, wearable technology or other 'Internet of Things' devices.

In 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 we 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. The key point is that you should be upfront with your users about your use of cookies. You should obtain consent 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.

Any attempt to gain consent that is bundled in terms and conditions will not be compliant.

Can we use 'cookie walls'?

A cookie wall – sometimes called a 'tracking wall' – requires users to 'agree' or 'accept' the setting of cookies before they can access an online service's content. This is also known as the 'take it or leave it approach'.

In some circumstances, this approach is inappropriate; for example, where the user or subscriber has no genuine choice but to sign up. This is because the UK GDPR says that consent must be freely given.

Further, Recital 43 of the UK GDPR states that:

> 'Consent is presumed not to be freely given if it does not allow separate consent to be given to different personal data processing operations despite it being appropriate in the individual case, or if the performance of a contract, including the provision of a service, is dependent on the consent despite such consent not being necessary for such performance.'

The ePrivacy Directive refers to conditional access to website content in Recital 25. This is sometimes used to justify using a cookie wall. It states:

> 'Access to specific website content may be made conditional on the well-informed acceptance of a cookie or similar device, if it is used for a legitimate purpose.'

However, when considering Recital 25, you should note that:

- 'specific website content' means that you should not make 'general access' subject to conditions requiring users to accept non-essential cookies – you can only limit certain content if the user does not consent; and
- the term 'legitimate purpose' refers to facilitating the provision of an information society service – ie, a service the user explicitly requests. This does not include third parties such as analytics services or online advertising.

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.

However, it should be noted that not all cookie tracking is necessarily intrusive or high risk. Furthermore, the UK GDPR is clear that the right to the protection of personal data:

- is not absolute;
- should be considered in relation to its function in society; and
- must be balanced against other fundamental rights, including freedom of expression and the freedom to conduct a business.

The key is that individuals are provided with a genuine free choice; consent should not be bundled up as a condition of the service unless it is necessary for that service.

Further reading – ICO guidance

Consent

Further reading – European Data Protection Board

The European Data Protection Board (EDPB), which has replaced the Article 29 Working Party (WP29), includes representatives from the data protection authorities of each EU member state. It adopts guidelines for complying with the requirements of the EU version of the GDPR.

For information about the meaning of Recital 25, read WP29's Working Document on cookie consent from 2013.

While these guidelines are no longer directly relevant to the UK regime and are not binding under the UK regime, they may still provide helpful guidance.

Can we pre-enable any non-essential cookies?

No. 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. By doing this, you are taking the choice away from the user.

Example

A website sets non-essential cookies on its landing page. Its cookie consent mechanism includes wording such as 'By continuing to use our website, you consent to our use of cookies'.

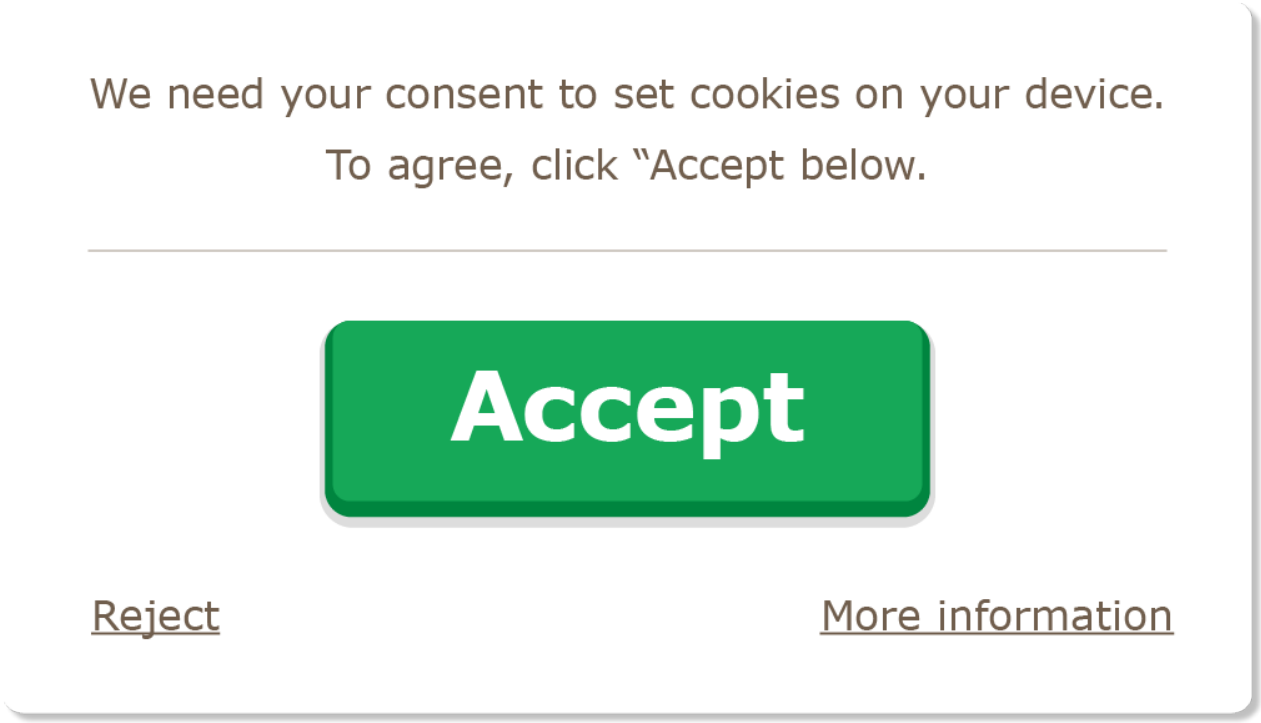
This does not represent valid consent, even if the mechanism also includes an 'OK' or 'Accept' button.

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 they want to accept or reject the cookies.

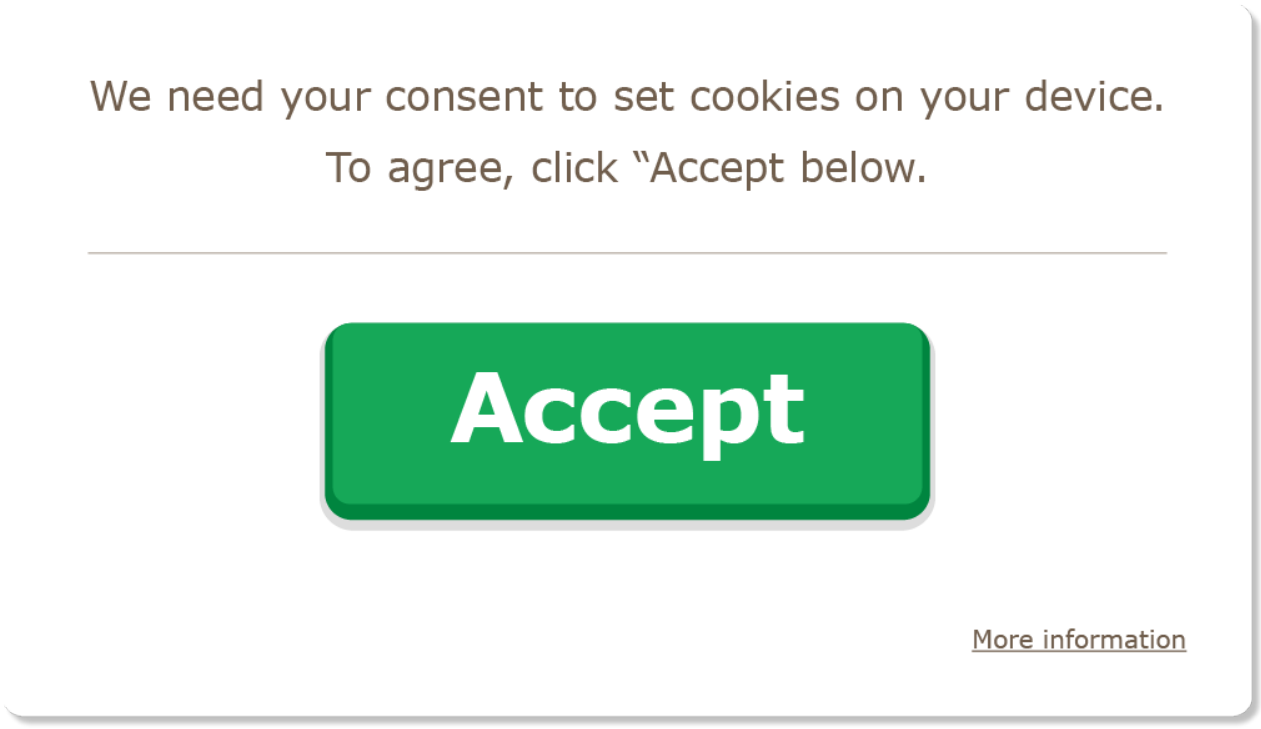
Depending on the circumstances, particularly the design of your consent mechanism and the wording you use in the information you provide, it is also likely that predetermining non-essential cookies could be considered as 'nudge behaviour' – ie, you are influencing the user to take a particular course of action.

Example

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.



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.



Where your online service must also comply with the ICO's code of practice on age-appropriate design – ie because it is likely to be accessed by a child – 'nudge behaviour' cannot be used.

At all times, the key is that you ensure you provide clear and comprehensive information to the user, and have an appropriate consent mechanism that meets the requirements of the UK GDPR.

Ultimately, users may be more likely to give their consent to non-essential cookies where they fully understand:

- what you use cookies for;
- how you have gone about seeking their consent;
- how you (and any third party) intends to use their data; and
- that you have provided them with appropriate control over their preferences.

This can also be a means of enhancing trust and confidence in your online service.

What if we use third-party cookies?

Your online service may allow third parties to set cookies on a user's device. For example, if you include content from a third party (eg from an advertising network or a streaming video service) this third party may read and write their own cookies onto users' devices.

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. In practice, it is obviously considerably more difficult for a third party who has less direct control on the interface with the user to achieve this. It is also important to remember that users are likely to address any concerns or complaints they have to the person they can identify or have the relationship with – in this case you, as

the company running the website. It is therefore in both parties' interests to work together.

If you are a third party wanting to set cookies, or you want to provide a product that requires the setting of cookies, you should include a contractual obligation into your agreements with web publishers. This can provide assurance that appropriate steps will be taken to provide information about the third party cookies and to obtain consent. However, you may need to take further steps, such as ensuring that the consents were validly obtained.

If you design and develop websites or similar technologies for other people you must also carefully consider the requirements of PECR and make sure the systems you design allow your clients to comply with the law. You must also ensure that when you design and develop new online services, or upgrade software, that you take into account both the requirements in PECR and broader data protection requirements, particularly in respect of Article 25 of the UK GDPR on data protection by design.

This is an approach whereby privacy and data protection compliance is designed into systems and services right from the start, rather than being bolted on afterwards or ignored.

Further reading – ICO guidance

Data protection by design

Obviously, the process of getting consent for third-party cookies is more complex and everyone has a part to play in making sure that the user is aware of what is being collected and by whom.

However, 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.

This is one of the most challenging areas in which to achieve compliance with PECR. The ICO continues to work with industry and other regulators to assist in addressing the difficulties and finding workable solutions.

Are analytics cookies exempt?

No. It is important to note that PECR does not distinguish between cookies used for analytics activities and those used for other purposes. Analytics cookies do not fall within the 'strictly necessary' exemption. This means you need to tell people about analytics cookies and gain consent for their use.

Analytics cookies are used so online services can collect information about how people access them – for example, the number of users on a website, how long they stay on the site for, and what parts of the site they visit. This is also sometimes known as 'web audience measurement'. This work is often done 'in the background'.

Whilst analytics can provide useful information for you, they are not part of the functionality that the user requests when they use your online service – if you didn't have analytics running the user could still be able to access your service. This is why analytics cookies aren't strictly necessary and do require consent.

There are two types of analytics cookies: first-party and third-party. Consent is necessary for first-party analytics cookies, even though they might not appear to be as intrusive as others that might track a

user across multiple sites or devices. You need to consider how you will explain your policies to users and make that information more prominent.

A number of services exist that provide an analytics function, and it could be easier for you to use these instead of building your own. However, it can be more difficult to obtain consent for third-party analytics cookies as there is no direct relationship between the third-party organisation and the user of your site. In these cases you need to ensure the information you provide to users about these cookies is absolutely clear and is highlighted in a prominent place – for example you can't just include it through a general privacy policy link.

If personal data is also processed through your use of a third-party analytics service, you need to take account of data protection requirements.

You should put measures in place to highlight the use of analytics cookies and to obtain agreement to set these cookies.

If the information collected about website use is passed to a third party this should be made absolutely clear to your users. It should also be clear what this third party does with this information. Depending on the specifics of your service, you may also offer users the ability to alter the settings of their account to limit the sharing of their information with third parties, including the analytics provider. (The analytics service may also provide this functionality, and you should consider enabling it where appropriate to do so.) In any case, the controls provided to the user should be prominently displayed and not hidden away.

Ultimately, you have to provide clear information to users about analytics cookies and to take steps to seek their consent. This is likely to involve making the argument to show users why these cookies are useful to them – but you must ensure if you do this you aren't leading the user to one option over another.

Although the ICO cannot rule out the possibility of formal action in any area, this may not always be the case where the setting of a first-party analytics cookie results in a low level of intrusiveness and low risk of harm to individuals. However you should also note that where you use first-party analytics cookies provided by a third party, this is not necessarily going to be the case.

Further reading – ICO guidance

Read the section on 'What happens if we don't comply?' for more information.

How do the exemptions apply to different types of cookies?

The exemptions in PECR relate to the purpose for which you store information, or gain access to information stored, on user devices. You are required to be clear with your users about these purposes when providing information and requesting consent, and if you have undertaken a cookie audit you should already know what these purposes are.

This section is not intended to provide an exhaustive list of how PECR's exemptions work for all types of cookies. It is an indicative list based on a number of common purposes that you may use cookies for.

Activity	Likely to meet an exemption?

User input	✓	**Yes, depending on purpose limitation.** If your online service uses a session cookie to track user input for specific functions of your service (eg a shopping basket or completing a form), then you can rely on the strictly necessary exemption provided that the cookie is only used for this purpose. This may not apply if the cookie is persistent.
Authentication	✓	**Yes, depending on purpose limitation.** If you use first-party session cookies for authentication purposes, you can rely on the strictly necessary exemption provided they are only used for this purpose. However, persistent login cookies are not exempt (as the user may not remember that they are logged in on a subsequent visit) and therefore consent is required in these cases. The cookie must only be used for authentication. If you also use the cookie for monitoring behaviour or tracking the user then consent is required.
Security	✓	**Yes, depending on purpose limitation.** First-party cookies used for security purposes can rely on the strictly necessary exemption; for example, cookies used to detect repeated failed login attempts. They can also have a longer duration than a session cookie. However, cookies that relate to the security of other online services besides your own require consent. This is because the functionality the user has requested relates to your service, not those of any others. If you use device fingerprinting techniques for a specific security purpose then you can also rely on the strictly necessary exemption. However, as with cookies, if the information is processed for secondary purposes - such as those relating to the security of online services the user has not requested - consent is required. This also applies where the information is processed for the purposes of fraud prevention, particularly in cases where multiple online services use a single fraud prevention service which processes information from visitors of all of those services.
Streaming content	✓	**Yes, depending on purpose limitation.** If your service is an online content provider that uses streaming media, then you can rely on the strictly

		necessary exemption for cookies that relate to the video or audio. This is because the streaming media forms part of the service that the user has requested. However, the exemption does not extend to cases where the cookie processes information that is not strictly necessary for the purposes of the streaming functionality, such as personalisation or usage monitoring. Additionally, where an online service merely includes streaming content hosted by a third-party online content provider (eg, where a website embeds YouTube videos, even those from its own YouTube channel), the exemption may not apply. If this applies to you, you will need to consider the circumstances carefully.
Network management	✓	**Yes, depending on purpose limitation.** If you use session cookies for load balancing purposes, you can rely on the communication exemption. This applies only where the cookies are for the sole purpose of identifying which server in the pool the communication will be directed to. Where you use device fingerprinting techniques for network management, you could also rely on the communication exemption provided that the use is solely for this purpose.
User preference	✓	**Yes, depending on purpose limitation.** Session cookies used to store a user's preference can rely on the strictly necessary exemption, provided they are not linked to a persistent identifier. The exemption may in some cases also apply to persistent cookies but the user must be given sufficient information in a prominent location - for example, cookies used as part of a cookie consent mechanism, which remember the user's cookie preferences over a period of time (eg 90 days), can be exempt. Alternatively, the act of interacting with the consent mechanism can be sufficient for consent to be obtained for any cookies relating to that mechanism, provided the user is given clear and comprehensive information as to the fact that a persistent cookie will be set on their device for the purpose of remembering their cookie consent preference. Where device fingerprinting techniques process information to optimise the site layout - such as

		where an online service uses responsive design, so that the site changes depending on the type of device - the strictly necessary exemption can apply. This would also apply to any third party services that are incorporated. However, the information accessed must be used solely for this purpose. Any secondary purposes mean the exemption would not apply and consent is required.
Social media plugins	**x**	**Consent required.** Where a user of your online service is also logged in to a social media platform, and your service includes plugins and other tools provided by that platform, they might expect to be able to use these plugins as part of their interaction with the social network. In such cases, the cookies that the plugins set on your service could be seen as strictly necessary for the functionality the user has requested. However, this would not apply to non-logged in users of that social media platform – be these users who have logged out, or users that are not members of that network. Consent is therefore required for any cookies that the social plugins set. Unless the plugins are configured only to set cookies on devices used by logged-in members of the social media platform, consent is likely to be required in all circumstances as you cannot assume that all of your visitors will also be members of whichever social networks you link to.
Social media tracking	**x**	**Consent required.** Where a social media plugin or other technology tracks users, be they members or non-members of that particular platform, for other purposes (including but not limited to online advertising, behavioural monitoring, analytics, or market research) the strictly necessary exemption would not apply. Any use of web beacons, tracking pixels, JavaScript code or similar technologies from a social media platform or any other third party is not exempt from the consent requirements. Additionally, there is no applicable lawful basis other than consent for social media platforms to process information about non-members of their networks through these technologies.

Online advertising	**x**	**Consent required.** If your service includes cookies used for the purposes of online advertising, you cannot rely on the strictly necessary exemption. Online advertising cookies are not exempt from PECR's consent requirements and never have been. This includes all third-party cookies used in online advertising, including for purposes such as frequency capping, ad affiliation, click fraud detection, market research, product improvement, debugging and any other purpose. Use of device fingerprinting techniques from advertising networks is also not exempt from the consent requirements. You should also note that your users are often unaware that this processing is taking place and that it involves creating profiles of users across different services over time to serve targeted advertising.
Cross-device tracking	**x**	**Consent required.** Where you use cookies or device fingerprinting techniques to link a user's account with a particular device or devices (eg, as part of the account profile, to provide a second authentication factor or to track users across multiple devices for any purpose – including advertising), consent is required. This is because this purpose is not strictly necessary to provide the functionality the user requests.
Analytics	**x**	**Consent required.** You are likely to view analytics as 'strictly necessary' because of the information they provide about how visitors engage with your service. However, you cannot use the strictly necessary exemption for these. Consent is required because analytics cookies are not strictly necessary to provide the service that the user requests. For example, the user can access your online service whether analytics cookies are enabled or not. If you use device fingerprinting for analytics instead of or alongside cookies, you should note that doing so is not exempt from the consent requirements either.

What if our users change their minds about cookies?

Once consent has been obtained, users or subscribers are able to withdraw that consent at any time. You should therefore ensure that your consent mechanism has the technical capability to allow users to withdraw their consent with the same ease that they gave it, otherwise it will not be compliant with the UK GDPR's consent requirements.

You must also provide information about how consent can be withdrawn, and how cookies that have already been set can be removed, eg in your consent mechanism or within your privacy or cookie policies.

The consequences of withdrawing that consent could be made clear, for example, by explaining the impact on the functionality of the website.

How often should we get consent?

You should ensure that any first time visitors to your website are provided with clear information about the cookies you use and are given choices and controls about any non-essential ones.

There are a range of reasons why you may need visitors to 'reconsent' to cookie settings. However, depending on the circumstances you may not need to ask for fresh consent each time someone visits. A number of factors will be involved, such as frequency of visits or updates of content or functionality.

An example of where you need to obtain fresh consent is when you are setting non-essential cookies from a new third party. This is because the consent that the user previously gave would apply only to those parties that you specified at the original time. When your service sets cookies from a new third party, you would need to ensure that users consent to this.

Importantly, the clear and comprehensive information you provide in your consent request should not include ambiguous or unclear references to 'partners' or 'third parties'. This would mean that the consent is invalid, as it is not specific and therefore the user is not fully informed.

How should we keep records of user preferences?

Some users will visit your website regularly and others will visit rarely, with a spectrum of others in between.

You therefore need to decide an appropriate interval between when you require users to select their preference (whether that is consent or rejection), and also decide when that preference expires (after which point users are given the option again).

At the same time, PECR isn't intended to inconvenience or unduly disrupt the experience of your users. You are not expected to repeatedly require your users to specify their preference as a matter of course, whether that results in consent for non-essential cookies or refusal.

These are issues that you will need to determine as the service provider.

Example

A website decides to use a cookie consent mechanism that enables the user to consent, or to reject, non-essential cookies. When users consent to the setting of these cookies, the website records this

preference in its own persistent cookie, which is stored on the users' devices and set to expire at a certain point in the future.

Provided the user visits again before the expiration date, they won't need to 'reconsent' to the cookies, because the site's preference cookie recognises that they consented previously. On the other hand, if the user visits infrequently then the cookie may expire before their next visit – meaning that they would need to consent again in the future.

The exact interval for the expiration a persistent cookie is a matter for you to consider, in relation to the circumstances of your online service and what you are seeking user consent for.

Additionally, if you use a third party consent mechanism and this records consents in digital form, you will need to ensure that this data is appropriately protected (and, if personal data is involved, that you have also considered any obligations under the UK GDPR – such as whether the third party is a processor or joint controller).

You should note that many 'off-the-shelf' consent mechanisms that use preference cookies may default to a certain expiration period, such as 90 days or so. Whilst using the default may be the simplest option you should nevertheless take the time to determine whether this interval is appropriate for you, and then document your conclusions.

Our guidance on consent gives more specifics about how you should go about recording consent, and how you should go about determining how long you should retain those records for.

Further reading – ICO guidance

Consent

How long should our cookies last?

This will depend on the purpose of the cookie. However, it is important that you consider cookie duration because this can affect the application of the exemptions in Regulation 6(4).

This also depends on the purpose you use the cookie for – so it is difficult to provide comprehensive guidance for each possible type of cookie. 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.

Example

An online service features user accounts on its website. To ensure that users are who they say they are, the online service uses an authentication cookie to recognise the user.

Once the user has logged out of the service (or closed their browser), the cookie is no longer

required and is therefore deleted once this takes place.

In this case there is no reason for the cookie to be persistent.

If you are incorporating tools into your online service that involve cookies, you should check whether these have a default duration. This may be appropriate in relation to the purpose of the cookie, but you should still assess this and change it if appropriate.

As a general rule, the exemptions in PECR are more likely to apply to session cookies – those that last until the user has closed their browser, or just slightly afterwards. This isn't always the case, however.

There are some clear cases where the duration of a cookie is wholly disproportionate. For example, 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.

What else do we need to consider?

In detail

What if our use of cookies changes?

If your cookie use changes significantly, then you will need to consider how this impacts on any consent that you have already gained.

For example, if you introduce a new cookie, or change the purposes of cookies already in use change after consent has been obtained, then your users will need to be made aware of these changes in order to allow them to make an informed choice about this new activity.

What about cookies set on websites that we link to?

Your online service may not be the only place where users and subscribers could have cookies set during their interactions with you.

For example, if you have a presence on social media platforms, then those platforms will set cookies on users' devices once they visit your pages there, eg 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.

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 joint data controller for this activity with the platform.

This remains the case even if the network only provides you with anonymised or aggregated statistical information, as in order to generate that information the platform will process personal data, firstly by recording what visitors do and then by then anonymising that information.

You should be aware that 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 about cookies set on overseas websites?

It is firstly important to note that if you are based in the UK you will be subject to the requirements of PECR even if your website is hosted overseas (eg, using cloud services based in the USA).

Although PECR does not have specific provisions regarding organisations operating outside the European Economic Area (EEA), where personal data is processed the GDPR applies. If your organisation is based outside Europe and you offer online services designed for the European market (eg that provide products or services to customers in Europe), you need to comply with the GDPR's requirements in respect of the information you provide to users as well as when, and how, you obtain consent.

So, where personal data is involved, if the user is not provided with clear and comprehensive information about the use of cookies then they cannot be said to be appropriately informed about the processing of their personal data – which is part of the fundamental data protection principle about fair, lawful and transparent processing.

When assessing whether the GDPR's territorial scope provisions apply to you, you should take account of:

- whether the processing relates to personal data of individuals in the EEA, and
- whether that processing also relates to the offering of goods and services or monitoring of behaviour.

Mere availability of a website to users within the EEA will not automatically be sufficient to bring that website in scope.

Example

An e-commerce website based outside the EEA offers users the ability to set up accounts and purchase products from any location in the world. Users can also list product prices in different currencies, including Pounds, Euros and other EEA currencies.

It is therefore clear that the products the site sells are intended to be offered to individuals within the EEA, and the site would be in scope of the GDPR.

Where the site uses cookies and similar technologies to process personal data, it would need to provide users in the UK and Europe with information about these cookies and comply with the rest of the GDPR.

A website may be available globally, and therefore accessible to individuals within the EEA, but this will not always mean it is specifically offering goods and services to those individuals. It will depend on the particular circumstances.

Example

An online news outlet based outside the EEA but accessible to individuals within the EEA may not be in scope of the GDPR, depending on its circumstances. The outlet may carry news reports relating to the EEA, but if this content is 'directed at' individuals within the outlet's own country or territory, rather than individuals in the EEA, then it will not be in scope of the GDPR even if those individuals can access the news reports online.

However, if the outlet intends to have a 'global' reach then it obviously means to offer its service to anyone, including EEA individuals; it will therefore need to consider whether the GDPR's territorial provisions apply to it, and the implications this has for providing cookie information and obtaining consent.

If you have a non-EEA website you can also take steps to demonstrate that you are not intending to offer goods and services to EEA individuals, for example:

- including specific references in your privacy information; or
- preventing EEA users from accessing your site, eg via IP address blocking.

The decision to undertake this activity is entirely down to you, but may provide an effective means of demonstrating that you do not intend to offer your service to individuals in the EEA.

Further reading – European Data Protection Board

The European Data Protection Board (EDPB), which has replaced the Article 29 Working Party (WP29), includes representatives from the data protection authorities of each EU member state. It adopts guidelines for complying with the requirements of the GDPR.

The EDPB has recently published guidelines on the territorial scope of the GDPR. These guidelines are currently subject to public consultation. We will update this link when the EDPB completes this work.

Can public authorities set cookies on their websites?

The requirements to provide clear and comprehensive information and obtain consent apply for anyone using cookies, whether or not you are a public authority. So, if you are a public authority that runs an online service – such as your website – the cookie rules apply to you as well.

What about other devices like mobiles, smart TVs, wearables, and the 'Internet of Things'?

In recent years, there has been ever-increasing usage of mobile devices such as smartphones and fitness bands, and internet-enabled appliances such as smart TVs and other so-called 'Internet of Things' devices such as home thermostats and connected vehicles. Generally, connected devices come under the definition of 'terminal equipment'.

Web services, often called web application programming interfaces (APIs) are typically used by mobile devices and other hardware. Since these services can also store or access information on the user's device just like any website, it is important to note that the cookie rules apply to all such devices where cookies or similar technologies are in use.

Here are some points to remember:

- A web API that sets cookies must comply with the cookie rules. In the field of mobile devices, this typically means that the mobile app accessing the web API is the obvious place to incorporate consent mechanisms, where applicable. It also means that users who access the web API using other means (eg a web browser) might not receive the same information and might need to be treated differently in order to avoid setting cookies without consent.
- In the same way that a website can make use of existing browser settings (as detailed in Regulation 6(3)(a) of PECR) to obtain consent, preference settings within a device's operating system may mature into a consent mechanism for app and web app developers.
- The limited, and sometimes non-existent, physical interfaces on some internet-connected devices pose challenges when trying to inform users about cookies and their purposes. Without being able to display information as part of a website itself, you need to consider alternative methods of informing users. These might include clear instructions packaged along with the device, information provided during product registration, or use of a companion mobile app to provide an interface so that information can be communicated and consent gained.

What happens if we don't comply?

The ICO's aim is to ensure organisations comply with the law. In cases where organisations refuse or fail to comply voluntarily the ICO has a range of options available for taking formal action where this is necessary.

Although the GDPR gives the ICO enhanced powers, the enforcement regime for PECR remains that which was in effect under the 1998 Data Protection Act – except where personal data is processed.

Where formal action is considered, perhaps because 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, any use of formal regulatory powers would be considered in line with the factors set out in the published Regulatory Action Policy.

More guidance on the circumstances in which the Information Commissioner will use enforcement powers, including what is considered a 'serious infringement', can be found in the ICO's civil monetary penalties guidance.

The Regulatory Action Policy 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.

The ICO cannot exclude the possibility of formal action in any area. However, 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. For example, the ICO is unlikely to prioritise first party cookies used for analytics purposes where these have a low privacy risk, or those that merely support the accessibility of sites and services, for regulatory action.

Further reading – ICO guidance

Read our Regulatory Action Policy and guidance on civil monetary penalties for more information.