Cookies and similar technologies

In brief...

You must tell people if you set cookies, and clearly explain what the cookies do and why. You must also get the user's consent. Consent must be actively and clearly given.

There is an exception for cookies that are essential to provide an online service at someone's request (eg to remember what's in their online basket, or to ensure security in online banking).

The same rules also apply if you use any other type of technology to store or gain access to information on someone's device.

In more detail...

- What is a cookie?
- What do we need to do to comply?
- What else is covered, apart from cookies?
- What information must we give users?
- What counts as consent?
- Do we need consent from the subscriber or from the user?
- Are there any exemptions?
- Do the rules still apply if the data is anonymous?
- Where can we get more information?
- How do these rules affect apps?
- Checklists

What is a cookie?

A cookie is a small text file that is downloaded onto 'terminal equipment' (eg a computer or smartphone) when the user accesses a website. It allows the website to recognise that user's device and store some information about the user's preferences or past actions.

What do we need to do to comply?

The rules on cookies are in regulation 6. The basic rule is that you must:

- tell people the cookies are there;
- explain what the cookies are doing and why; and
- get the person's consent to store a cookie on their device.

As long as you do this the first time you set cookies, you do not have to repeat it every time the same person visits your website. However, bear in mind that devices may be used by different people. If there is likely to be more than one user, you may want to consider repeating this process at suitable intervals.

You may also need to obtain fresh consent if your use of cookies changes over time.

What else is covered, apart from cookies?

Although this guide focuses on cookies, regulation 6 actually applies to anyone who stores information on a user's device or gains access to information on a user's device, in either case by any method.

This means the same rules apply to any similar technologies – such as Local Shared Objects (sometimes called Flash cookies) – and can also cover other types of technology, including apps on smartphones, tablets, smart TVs or other devices.

These rules also outlaw spyware or any similar covert surveillance software that downloads to a user's device and tracks their activities without their knowledge.

What information must we give users?

PECR do not set out exactly what information you must provide or how to provide it – this is up to you. The only requirement is that it must be "clear and comprehensive" information about your purposes. You must explain the way the cookies (or other similar technologies) work and what you use them for, and the explanation must be clear and easily available. Users must be able to understand the potential consequences of allowing the cookies. You may need to make sure the language and level of detail are appropriate for your intended audience.

This is similar to the transparency requirements of the UK GDPR (privacy notices).

Further Reading

For further information, see our detailed guidance on cookies and the section of the Guide to the UK GDPR on the right to be informed.

What counts as consent?

To be valid, consent must be freely given, specific and informed. It must involve some form of unambiguous positive action – for example, ticking a box or clicking a link – and the person must fully understand that they are giving you consent. You cannot show consent if you only provide information about cookies as part of a privacy policy that is hard to find, difficult to understand, or rarely read.

Similarly, you cannot set non-essential cookies on your website’s homepage before the user has consented to them.

Consent does not necessarily have to be explicit consent. However, consent must be given by a clear positive action. You need to be confident that your users fully understand that their actions will result in specific cookies being set, and have taken a clear and deliberate action to give consent. This must be more than simply continuing to use the website. To ensure that consent is freely given, users should have the means to enable or disable non-essential cookies, and you should make this easy to do.

You should take particular care to ensure clear and specific consent for more privacy-intrusive cookies, such as those collecting sensitive personal data such as health details, or used for behavioural tracking. The ICO will take a risk-based approach to enforcement in this area, in line with our regulatory action policy.

For more advice on obtaining consent, including the rules on browser settings, see our cookies guidance and our consent guidance.

Further Reading

For further information, see our detailed guidance on cookies, as well as our guidance on consent in the Guide to the UK GDPR.

Do we need consent from the subscriber or from the user?

Regulation 6 states that consent should be obtained from the subscriber or user.

In practice you may not be able to tell who is the subscriber and who is a user – which means you may not be able to distinguish between consent provided by the subscriber and by the user. The key will be that valid consent has been provided by one of them.

PECR does not say whose wishes should take precedence if they are different. If there appears to be a conflict – for example, if a subscriber or user previously consented but now the current user of the same device objects – it would seem sensible to rely on the most recent indication. This would mean you always respect the current user’s preferences, even if you cannot be sure of the subscriber’s preferences.

Further Reading

For further information, see our detailed guidance on cookies.

Are there any exemptions?

There are two exemptions which apply where:

- the cookie is for the sole purpose of carrying out the transmission of a communication over an electronic communications network; or

- the cookie is strictly necessary to provide an 'information society service' (eg a service over the internet) requested by the subscriber or user. Note that it must be essential to fulfil their request – cookies that are helpful or convenient but not essential, or that are only essential for your own purposes, will still require consent.

This means you are unlikely to need consent for:

- cookies used to remember the goods a user wishes to buy when they add goods to their online basket or proceed to the checkout on an internet shopping website;
- session cookies providing security that is essential to comply with data protection security requirements for an online service the user has requested – eg online banking services; or
- load-balancing cookies that ensure the content of your page loads quickly and effectively by distributing the workload across several computers.

However, it is still good practice to provide users with information about these cookies, even if you do not need consent.

Further reading

For further information, see our cookies guidance.

You may also want to refer to the opinion adopted by European data protection authorities in June 2012 (Article 29 Working Party opinion 04/2012), which clarifies that some usage of session-ID cookies, multimedia cookies, and user interface customisation cookies (eg language-preference cookies) is likely to fall within the information society services exemption.

Although this publication refers to the requirements of the e-privacy Directive and the old EU Data Protection Directive (which preceded the EU and UK versions of the GDPR), it is also useful for understanding the requirements of PECR.

Do the rules still apply if the data is anonymous?

Yes. Although cookies that process personal data give rise to greater privacy and security risks than those that process anonymous data, PECR apply to all cookies.

If your cookie data is not anonymous, note that you will also need to comply with the Data Protection Act and the UK GDPR. You may need to carry out a data protection impact assessment (DPIA). You may actually need to consider whether you could use anonymised data instead, in order to comply with the data protection principles (which require personal data to be adequate, relevant and not excessive). This is likely to be particularly relevant where you are not using the data to provide a service to the user – for example, if you are simply counting visitors to a website.

At the same time, you should be aware that the creation of anonymous information may involve processing of personal data – for example, to generate aggregate statistics based on user interaction. This processing would therefore be covered by the GDPR.

See our separate Guide to UK GDPR for more information.

Where can we get more information?

For more detailed information and practical advice on this topic, see our guidance on cookies.

The ICO will continue to take a risk-based approach to enforcement in this area, taking into account the level of intrusion, the efforts made to provide clear information and get consent, and consumer concern. You can find more about the action we are taking on cookies on the Enforcement section of the ICO website.

How do these rules affect apps?

Apps store information on smart devices, and some apps may also access information on the device (eg contacts or photos). App developers should therefore provide clear information to users about what the app does, and exactly how it uses their information, **before** users click to install the app. It is also important to consider user privacy controls and avoid switching optional features on by default. This ties in closely with the requirements of the Data Protection Act and the UK GDPR.

Further reading – ICO guidance

For more information on how to comply, see our separate guidance Privacy in mobile apps. Although written under the 1998 Act, it may still assist you.

Checklists

Understanding cookies

☐ We understand what cookies are and what they can be used for.

☐ We know the difference between session cookies and persistent cookies.

☐ We know the difference between first party and third party cookies.

☐ We understand what ‘similar technologies’ are and how PECR applies to them.

Auditing our use of cookies

☐ We know what cookies our online service either already uses or intends to use.

☐ We have removed any cookies that we don’t need.

☐ We have confirmed the purposes of each cookie.

☐ We identify what information each cookie processes, including whether they are linked to other information we hold about our users or otherwise involve processing personal data.

☐ Where personal data is involved, we have ensured that we process this data in line with the requirements of the UK GDPR.

☐ We have confirmed whether our cookies are session or persistent cookies.

☐ We have confirmed whether our cookies are first party or third party cookies.

☐ We have appropriate arrangements in place for the use of any third-party cookies, including what information they share with any third party, how it is shared, and what our users are told.

☐ We have established how long our cookies last and that this duration is appropriate.

☐ We have identified those cookies that are strictly necessary, and those that are not.

Information about cookies

☐ We have ensured that we provide clear and easy to understand information about the cookies we use.

☐ We have ensured that our information is comprehensive and covers all the cookies we use.

Consent for cookies

☐ We have implemented a consent mechanism that allows users of our online service to control the setting of all cookies that are not strictly necessary.

☐ We ensure that our consent mechanism ensures the consent we obtain is in line with the UK GDPR's requirements.

☐ We keep any records of cookie consent for an appropriate period of time.

Documenting and reviewing our cookie use

☐ We have documented all of the above.

☐ We have built in an appropriate review period.