

Guidance on the use of storage and access technologies

Guidance on the use of storage and access technologies	6
Contents	6
About this guidance	6
What are storage and access technologies?	6
What are the PECR rules?	7
What are the exceptions?	7
How do the PECR rules relate to the UK GDPR?.....	7
How do we comply with the PECR rules?	7
How do we manage consent in practice?	8
How do the rules apply to online advertising?.....	8
What happens if we don't comply?	8
Glossary	8
About this guidance	9
What's new	9
April 2026 update:.....	9
Why have you produced this guidance?	11
Who is it for?	11
What does it cover?	11
What doesn't it cover?	11
What are storage and access technologies?	12
At a glance	12
In detail	12
What technologies does PECR apply to?	12
Cookies.....	13
Tracking pixels.....	13
Link decoration and navigational tracking	14
Device fingerprinting	15
Web storage	16
Scripts and tags	17
Using storage and access technologies in different contexts	18
What is the difference between 'first-party' and 'third-party' storage and access technologies?.....	18
What is the difference between 'session' and 'persistent' storage?..	20
What is the difference between 'client-side' and 'server-side'?	21
What are the PECR rules?	23

At a glance	23
In detail	23
What does PECR say about storage and access technologies?	23
Who are subscribers and users?	24
What is terminal equipment?	24
What does ‘clear and comprehensive information’ mean?	24
What does ‘consent’ mean?	25
Do the rules only apply to websites and web browsers?	26
Do the rules apply to our internal network?	27
Do the rules apply to public authorities?	27
Do the rules apply to services based outside the UK?	27
What if children are likely to access our online service?	29
What are the exceptions?	30
At a glance	30
In detail	30
Do all storage and access technologies require consent?	30
What is the ‘communication’ exception?	31
What is the ‘strictly necessary’ exception?	32
What activities are likely to meet this exception?	33
What is the ‘statistical purposes’ exception?	37
What activities are likely to meet the exception?	37
Can we use a third-party analytics service?	40
What is the ‘appearance’ exception?	42
What is the ‘emergency assistance’ exception?	44
What does ‘a simple means of objecting’ mean?	45
How do the PECR rules relate to the UK GDPR?	47
At a glance	47
In detail	47
What is the relationship between PECR and the UK GDPR?	47
What does the UK GDPR say about storage and access technologies?	48
How does PECR consent fit with the lawful basis requirements of the UK GDPR?	49
What does PECR say about subsequent processing?	50
How do we comply with the PECR rules?	52

At a glance	52
In detail	52
Who is responsible for compliance?	52
How do we consider PECR when designing a new online service?	53
What do we need to consider if we use someone else’s technologies on our online service?	54
How do we tell people about the storage and access technologies we use?	55
How do we tell people about storage and access technologies set on websites that we link to?	56
Can we pre-enable any non-exempt storage and access technologies?	58
How long can we store or access information for?	58
What is an audit and how can we do one?	60
How do we manage consent in practice?	62
At a glance	62
In detail	62
When do we need to get consent?	63
Who do we need consent from?	63
How do we request consent?	64
Can we use pop-ups and similar techniques?	65
Our expectations for consent mechanisms	65
<input type="checkbox"/> Our consent mechanism makes it as easy to refuse consent as it is to accept.	66
<input type="checkbox"/> Our consent mechanism requires a positive action to indicate opt-in from the user, before non-exempt storage and access technologies are set.	67
<input type="checkbox"/> Our consent mechanism functions as intended. Storage and access technologies are only set when valid consent is gathered, or when they meet an exception.	67
<input type="checkbox"/> Our consent mechanism includes granular options for different purposes.	68
<input type="checkbox"/> Our consent mechanism informs users about the identities of all third parties their information will be shared with if they grant consent. Users are able to control any information shared with individual third parties.	68

<input type="checkbox"/> Our consent mechanism informs users about how they can revisit their preferences.....	69
<input type="checkbox"/> Our consent mechanism does not incorrectly use legitimate interests as a lawful basis.	69
Can we rely on settings-based consent?	70
Can we rely on feature-led consent?	70
Can we rely on browser settings and other control mechanisms for consent?	70
Can we use ‘terms and conditions’ to gain consent?.....	71
Can we bundle consent requests?	71
How often do we need to request consent?	72
What if our use of storage and access technologies changes?	73
Can we use the same storage and access technology for multiple purposes?	74
How do we keep records of user preferences?.....	75
What if a user withdraws their consent?	76
How do the rules apply to online advertising?.....	78
At a glance	78
In detail	78
Do we need consent for online advertising?	78
Does advertising measurement require consent?.....	79
What types of online advertising can we use?	80
Can we use ‘cookie walls’ or ‘consent or pay’ models?	81
What happens if we don’t comply?	83
What happens if we don't comply	83
Glossary	84
Glossary.....	84

Guidance on the use of storage and access technologies

29 April 2026 - we have finalised this guidance following two consultations on the draft guidance: the significant update to the previous detailed cookies guidance in December 2024, and the consultation on the changes to PECR following the Data (Use and Access) Act in July 2025. [We have summarised the responses to both consultations.](#)

We have added two new sub-chapters: “what does a ‘a simple means of objecting’ mean?” and “can we use the same storage and access technology for multiple purposes?”

There are minor changes to the content where we have sought to provide further clarity where requested in the consultation.

07 July 2025

- We have updated this draft guidance to reflect changes to PECR following the Data (Use and Access) Act.
- We have added a new chapter “what are the exceptions?” to explain the exceptions to the prohibition on storing or accessing information on people’s devices.
- There are other minor changes throughout the guidance to reflect the updated rules.
- Outside of the indicated updates, this guidance is still in draft form as per the December 2024 update. We will finalise it following the second consultation on the new chapter.

20 December 2024 - this guidance was published

Contents

[About this guidance](#)

- [What’s new?](#)
- [Why have you produced this guidance?](#)
- [Who is it for?](#)
- [What does it cover?](#)
- [What doesn’t it cover?](#)

[What are storage and access technologies?](#)

- [What technologies does PECR apply to?](#)
- [Cookies](#)

- Tracking pixels
- Link decoration and navigational tracking
- Device fingerprinting
- Web storage
- Scripts or tags
- Using storage and access technologies in different contexts

What are the PECR rules?

- What does PECR say about storage and access technologies?
- Who are subscribers and users?
- What is terminal equipment?
- What does ‘clear and comprehensive information’ mean?
- What does ‘consent’ mean?
- Do the rules only apply to websites and web browsers?
- Do the rules apply to our internal network?
- Do the rules apply to public authorities?
- Do the rules apply to services based outside the UK?
- What if children are likely to access our online service?

What are the exceptions?

- Do all storage and access technologies require consent?
- What is the ‘communication’ exception?
- What is the ‘strictly necessary’ exception?
- What is the ‘statistical purposes’ exception?
- What is the ‘appearance’ exception?
- What is the ‘emergency assistance’ exception?
- What does ‘a simple means of objecting’ mean?

How do the PECR rules relate to the UK GDPR?

- What is the relationship between PECR and the UK GDPR?
- What does the UK GDPR say about storage and access technologies?
- How does PECR consent fit with the lawful basis requirements of the UK GDPR?
- What does PECR say about subsequent processing?

How do we comply with the PECR rules?

- Who is responsible for compliance?
- How do we consider PECR when designing a new online service?
- What do we need to consider if we use someone else’s technologies on our online service?

- How do we tell people about the storage and access technologies we use?
- How do we tell people about storage and access technologies set on websites that we link to?
- Can we pre-enable any non-exempt storage and access technologies?
- How long can we store or access information for?
- What is an audit and how can we do one?

How do we manage consent in practice?

- When do we need to get consent?
- Who do we need consent from?
- How do we request consent?
- Can we use pop-ups and similar techniques?
- Our expectations for consent mechanisms
- Can we rely on settings-based consent?
- Can we rely on feature-led consent?
- Can we rely on browser settings and other control mechanisms for consent?
- Can we use ‘terms and conditions’ to gain consent?
- Can we bundle consent requests?
- How often do we need to request consent?
- What if our use of storage and access technologies changes?
- Can we use the same storage and access technology for multiple purposes?
- How do we keep records of user preferences?
- What if a user withdraws their consent?

How do the rules apply to online advertising?

- Do we need consent for tracking and profiling for online advertising?
- Does advertising measurement require consent?
- What types of online advertising can we use?
- Can we use ‘cookie walls’ or ‘consent or pay’ models?

What happens if we don’t comply?

Glossary

About this guidance

What's new

April 2026 update:

- We have finalised this guidance following two consultations on the draft guidance: the significant update to the previous detailed cookies guidance in December 2024, and the consultation on the changes to PECR following the Data (Use and Access) Act in July 2025. [We have summarised the responses to both consultations.](#)
- We have added two new sub-chapters: “what does a ‘simple means of objecting’ mean?” and “can we use the same storage and access technology for multiple purposes?”
- There are minor changes to the content where we have sought to provide further clarity where requested in the consultation.

July 2025 update:

- We have updated this draft guidance to reflect changes to PECR following the Data (Use and Access) Act.
- We have added a new chapter “what are the exceptions?” to explain the exceptions to the prohibition on storing or accessing information on people’s devices.
- There are other minor changes throughout the guidance to reflect the updated rules.
- Outside of the indicated updates, this guidance is still in draft form as per the December 2024 update. We will finalise it following the second consultation on the new chapter.

Below we outline the changes at chapter level so past readers of the detailed cookies guidance can navigate the changes.

What are storage and access technologies?

This is a pre-existing chapter with new content to explain other storage and access technologies covered by PECR in more detail, alongside cookies.

What are the PECR rules?

This is a pre-existing chapter with some changes to the content, including added detail and new examples. This chapter now includes some sub-sections that were previously contained elsewhere in the guidance.

What are the exceptions?

This is a new chapter to explain the five exceptions to the prohibition on storing or accessing information on people's devices.

How do the PECR rules relate to the UK GDPR?

This is a pre-existing chapter with minor changes to the content.

How do we comply with the PECR rules?

This is a pre-existing chapter which has been split into multiple chapters. This chapter includes refreshed examples and minor changes to the text of existing sub-sections, including some new policy lines.

How do we manage consent in practice?

This is a new chapter with some content from the previous 'How do we comply with the PECR rules?' chapter. It also includes new content to reflect our expectations for requesting consent, with examples of good and bad practice consent mechanisms.

How do the rules apply to online advertising?

This is a new chapter with mostly new content to provide clarity on how the rules apply to online advertising.

What happens if we don't comply?

This is a pre-existing chapter with changes to reflect the changing PECR enforcement regime.

Glossary

This is a new resource.

December 2024 update:

- This guidance is a significant update to the detailed cookies guidance. It provides added clarity on our expectations for using other storage and access technologies as well as cookies.
- We have rewritten the guidance using 'must', 'should', or 'could' language to provide regulatory clarity to readers.
- The guidance reflects recent case law and our positions on key topics, including on our expectations for online advertising.

Why have you produced this guidance?

This guidance explains how the Privacy and Electronic Communications Regulations (as amended) (PECR), and where relevant data protection law, apply when you use technologies that store information, or access information stored, on someone's device (eg a computer or mobile phone).

Read it to understand the law and our recommendations for good practice.

Who is it for?

This guidance is aimed at providers of online services, including web or app developers, who need a deeper understanding of how PECR, and where relevant data protection law, apply to the use of storage and access technologies.

What does it cover?

The technologies PECR applies to include (but is not limited to):

- cookies;
- tracking pixels;
- link decoration and navigational tracking;
- local storage;
- device fingerprinting; and
- scripts and tags.

The guidance also covers the UK GDPR, where the use of these technologies involves processing personal data.

What doesn't it cover?

Other areas of PECR outside of regulation 6, except where relevant to the use of storage and access technologies.

Wider compliance obligations with the Data Protection Act (DPA) and UK GDPR when using storage and access technologies, except for where they are relevant to PECR requirements.

Must, should, could - using this guidance to comply

<https://ico.org.uk/about-the-ico/must-should-could-using-this-guidance-to-comply/>

What are storage and access technologies?

At a glance

- PECR applies to any technology that stores information, or accesses information stored, on a subscriber's or user's 'terminal equipment'.
- PECR allows you to use storage and access technologies in particular circumstances, or with valid consent from the user.
- The rules apply to any use of these technologies, including on mobile apps and connected devices.
- Where the information stored or accessed is personal data, the UK GDPR also applies.

In detail

- [What technologies does PECR apply to?](#)
- [Cookies](#)
- [Tracking pixels](#)
- [Link decoration and navigational tracking](#)
- [Device fingerprinting](#)
- [Web storage](#)
- [Scripts and tags](#)
- [Using storage and access technologies in different contexts](#)

What technologies does PECR apply to?

PECR applies to any technology that stores information, or accesses information stored, on a subscriber's or user's 'terminal equipment'. This includes, but is not limited to:

- cookies;
- tracking pixels;
- link decoration and navigational tracking;
- web storage;
- fingerprinting techniques; and
- scripts and tags.

This guidance uses the term 'storage and access technologies' to refer to these. PECR allows you to use storage and access technologies in particular circumstances, or with valid consent from the user. The rules are explained in the '[What are the rules?](#)' section.

The rules apply to any use of these technologies, including in web browsers, mobile apps and connected devices. For example, a mobile app developer might wish to store information on a user's device, or access data from that device. These services can lead to storage or access of information on the user's device just like any website, so these rules will still apply.

The terms 'subscriber', 'user' and 'terminal equipment' are explained in the 'What are the rules?' section.

Cookies

Cookies are small text files generated by a web server responding to a request from a website. The user's device can store cookies (eg via their web browser) and send the information back when they next make a request to the same web server.

Cookies are widely used to make websites work, or work more efficiently, and to provide information to the website operator. For example, they can be used for:

- recognising a user's device;
- remembering what's in a shopping basket when shopping for goods online;
- supporting users to log in to a website or remembering they are logged in; or
- analysing traffic to a website and how users interact with the website.

They can also be used for other purposes, such as tracking users' browsing behaviour.

Tracking pixels

Tracking pixels are small pieces of code, usually an image file, embedded into a piece of content like a website or an email. Their purpose is to create a communication between the user's client (eg a web browser) and a server. The server can then identify information, such as when a user has viewed a webpage or opened an email.

Example

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

The majority of electronic mail marketing is governed by regulation 22 of PECR, but where tracking pixels store information (or gain access to information stored) on a user's device, regulation 6 applies to this processing.

Example

An organisation promotes their products online by using an affiliate marketing platform. The organisation integrates the affiliate platform's tracking pixel into the HTML of the order confirmation page. This allows the organisation to accurately attribute a sale to a particular affiliate marketing partner.

If a user visits the organisation's website after being redirected from an affiliate partner's website, information about the partner will be stored in the user's browser. For example, the time stamp for the click and an ID linked to the affiliate partner's site.

When a user completes a purchase on the organisation's site, their browser loads the order confirmation page and requests the pixel image from the affiliate platform's server. This request will append key information about the sale such as the order reference and transaction amount. Information previously stored about the affiliate partner is accessed from the user's browser and attached to the request.

This use of a tracking pixel involves storing information on a user's device and later accessing this information to share with a third party. Therefore regulation 6 applies.

Link decoration and navigational tracking

Regulation 6 applies where link decoration and navigational tracking techniques involve storage of, or access to, information on a device, or both. The key consideration for compliance is the purpose the techniques are used for.

Link decoration refers to the practice of adding extra information to the URL in a link that someone clicks on. This doesn't change the destination of the link, but provides a way to pass additional information to the destination site beyond what is essential to navigate to the page that the user wants to visit.

This extra information is generated:

- statically (eg by being attached to a URL when a link is created); or
- dynamically (eg through the use of JavaScript code).

When a user navigates to the webpage via the URL, the browser loads the requested resource. It may also involve storage or access of other information.

Online services often use link decoration to identify the origin of their inbound source of traffic (eg a specific email campaign).

Example

An e-commerce site emails its customers providing a URL to an article about its new product, available at <https://www.example.com/article>.

When the recipient clicks on the URL from the email they received, they are taken to:

https://www.example.com/article?referrer_source=emailnewsletter

However, this technique can also be used to pass tracking information around the web.

Navigational tracking is where link decoration is used to identify that a user of one site is the same person as a user on another site. For example, by adding a user ID to a URL. The same user ID may also be stored in a cookie or local storage, which can then be accessed to identify the user.

Example

As part of a marketing campaign, an advertiser places adverts on multiple social media platforms. They want to know how many sales originate from each platform. They also want to re-target users on each platform who have clicked on an advert but did not go on to make a purchase.

While scrolling on a social media platform, a user clicks on a relevant URL embedded in an advert and navigates to the advertiser's website. The social media platform adds a unique user ID to the URL when a user clicks on the advertiser's advert. The advertiser stores the unique identifier in a first-party cookie.

The user leaves the advertiser's website having viewed an item but without making a purchase. The advertiser uses the information passed from the social media site via the link decoration to re-target adverts about that item to that user on the same social media platform.

Regulation 6 applies.

Device fingerprinting

Device fingerprinting, such as browser fingerprinting techniques, involves collecting pieces of information about a device's software or hardware. These can be combined to uniquely identify a particular device.

Organisations may sometimes use device fingerprinting in the belief that regulation 6 does not apply to this process. However, it applies where fingerprinting stores information, or accesses information stored, on a device.

Examples of the information elements that fingerprinting techniques 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, external or both).

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

Example

An online service uses device fingerprinting for detecting fraudulent account creation and use of login credentials.

It involves collecting hardware information, browser information, location information and the IP address. This information is sent to a third-party security provider which probabilistically identifies a device using this information, to identify whether the activity is fraudulent.

Regulation 6 applies.

Example

A retailer collects email addresses from visitors to its website when they register for its newsletter or make a purchase. It uses this email address to re-target its visitors with adverts for its products on other websites.

The retail site embeds a tag on the webpage from an identity vendor which accesses and hashes the email address on the page when collected. This hashing technique generates a value which is then stored in a first-party cookie on the user's browser. Later the identity vendor helps the retail website's advertising and social media partners to match this hashed value with additional information to enable the retargeting of that user.

Even though the full email address is 'masked', an identifier is created for the purpose of processing information relating to the user, regardless of whether the original email address or other personal data can be inferred from it.

Regulation 6 applies. The UK GDPR also applies, as this processing involves personal data.

Web storage

Web storage is another way in which online services can store information, or access information stored, on someone's device. It involves websites storing data in someone's browser. It's also known as 'local storage', 'HTML5 storage' or 'DOM storage'.

Web storage involves a standard API that browsers include, known as the web storage API. There are two types of storage:

- 'localStorage', where the data may be stored permanently unless removed; and
- 'sessionStorage', where the data is stored only for the duration of the user's visit to a webpage.

The main differences between web storage and a technology like cookies are that:

- web storage allows more data to be stored in the browser; but
- the data is not transferred to a server (unless this is done manually).

In some situations, information may be generated as part of the general function of the device's software or hardware. PECR may not apply when that information, or information derived from it, is not accessed by an outside entity and stays on the device.

Example

A website wants to increase the value of the digital advertising it displays. It decides to integrate a service on its site that helps segment its website visitors into audiences and categories relevant to potential advertisers.

Now, when a user visits the website, the new service uses information obtained from the web page and the user's activity to understand if the user can be categorised into a particular audience category. When the information on the web page aligns to a pre-defined audience segment (eg 'sport'), the service stores this information in the browser's local storage.

Later, the user visits another page on the same site where the website owner has chosen to display an advert. Here, the service accesses the audience category previously recorded in localStorage and passes them to the advertiser interested in displaying a digital advert to a particular audience.

Regulation 6 applies.

Further reading

[HTML Standard \(whatwg.org\)](https://whatwg.org/html) (A web document that explains 'localStorage' and 'sessionStorage').

Scripts and tags

Online services can add pieces of JavaScript code, often referred to as ‘scripts’ or ‘tags’, to web pages to collect additional information about visitors to their service. When a user accesses a web page, their browser interprets the instructions included in the script and executes them. While scripts can be used for many purposes, ‘tags’ often refers to a JavaScript ‘snippet’ included specifically to gather data about a website's visitors.

To record and track information about a user, tags often involve the use of other storage and access technologies, such as cookies, local storage or device fingerprinting techniques.

Regulation 6 of PECR applies whenever the use of scripts and tags accesses or stores information on a user’s device — whether or not this is in conjunction with other storage and access technologies.

Organisations commonly work with a range of technologies and third-party providers when operating their services. To reduce complexity, they may use a ‘tag management system’ or ‘tag manager’ so they can add, edit or remove tags centrally.

Server-side tags can further reduce the amount of tag activity on a user's device, improving page loading times. Here, data relating to the user's activity on a site is sent to the tag manager's server before a decision is made about what data will be sent to each individual partner.

Where the information stored or accessed is personal data, the UK GDPR also applies.

Using storage and access technologies in different contexts

Storage and access technologies can be deployed in different contexts. The most common examples are:

- ‘first-party’ or ‘third-party’;
- ‘session’ or ‘persistent’; and
- ‘client-side’ or ‘server-side’.

It is important to understand that these contexts don’t necessarily impact whether regulation 6 applies. The key consideration is whether the technology stores or accesses information on a device and the purposes for which it does so.

What is the difference between ‘first-party’ and ‘third-party’ storage and access technologies?

Many uses of storage and access technologies differentiate between the concepts of ‘first party’ and ‘third party’. However, these terms can mean different things depending on the circumstances in which you use them.

The terms have no inherent meaning in PECR or UK GDPR. The PECR rules apply to any technology you use to store information, or access information stored, in someone’s device — whether in a first-party context or a third-party context.

The concepts are more relevant to web standards development and online practices.

The classic distinction usually relates to web standards terminology, where:

- **‘first party’** means the website the user is visiting (eg the domain/URL shown in the browser’s address bar); and
- **‘third party’** means a domain other than the one the user is visiting (eg cookies, code or other technologies from other websites, which allow the third party to store or access information on the device).

The most well-known example of this is with cookies, which may be first-party cookies or third-party cookies.

Online services commonly use third-party cookies. For example, when they incorporate resources hosted elsewhere, such as images, social media plugins or advertising.

However, third-party cookies can also link people’s activity across different sites and devices (ie web and cross-device tracking). This presents specific privacy risks, particularly when users may not know it is happening. Over time, software applications like web browsers have implemented limitations on the use of third-party cookies. These include providing user controls such as ‘tracking protection’ features and restricting or blocking third-party cookies from being set.

In some cases, this has led to the resources previously delivered by a third-party cookie being delivered via a first-party cookie — even where the resource itself is still external to the online service the user interacts with. This, alongside the use of communications at the server level, further complicates use of the terms.

Ultimately, whether a storage and access technology is classed as ‘first-party’ or ‘third-party’ is not the main consideration for data protection and privacy purposes. Instead, what’s primarily relevant is:

- who is responsible for the storage or access on terminal equipment, which in most cases is the service provider; and
- the purpose(s) of the storage or access.

Example

An organisation has a presence on a social media network. As part of its marketing strategy, the organisation wants to identify which users of its website are also members of the social media network so that it can promote its products and services to them on that platform.

The social media network provides a number of targeting tools for these purposes. These include a JavaScript snippet that the organisation can add either to the header code of its website (so that it records visitor activity across all pages), or to specific pages or sections of the site.

Using the tool leads to information about website visitors being disclosed to the social media network. This identifies visitors who are members of the social media network.

The organisation can deploy the tool in both the first-party and third-party contexts.

In the first instance, a visitor's browser recognises the tool as something delivered from the organisation's domain. In the second, the browser recognises it as something delivered from the social media network's domain.

However, the organisation's choice to deploy the tool in one context or the other doesn't change the fact that it may result in the storage or access of information on the devices of people visiting its website.

As such, regulation 6 applies and the organisation must obtain prior consent to use the tool.

Further reading

[RFC 6265](#), the W3C document that defines the HTTP cookie

What is the difference between 'session' and 'persistent' storage?

Storage and access technologies can last for different periods of time, depending on the choices you make when setting them. They can be:

- **session** storage, which generally expires when someone closes their browser or shortly afterwards; or
- **persistent** storage, where the information is stored between browser sessions and can therefore have a longer duration.

This is not an absolute rule. For example, some session cookies can be restored by the browser in the next session, and effectively last indefinitely. Similarly, data can be removed from persistent storage.

The purpose of the technology can sometimes determine whether the storage is session or persistent. For example:

- session storage is generally used for things that don't need to be stored for a long period of time (eg cookies that remember what someone has put in their shopping basket); and
- persistent storage is generally used for things like remembering someone's preferences between visits to an online service (eg a preference cookie).

As the online service provider, you are responsible for making decisions about the duration of storage and access technologies on your site, such as whether persistent storage is necessary for your purpose.

The '[How long can we store information for?](#)' section contains more information about how to make these decisions.

What is the difference between 'client-side' and 'server-side'?

In web development, the terms 'client' and 'server' refer to who is making and responding to requests for information over the internet.

A common example is with HTTP requests and responses. When someone clicks a link on a web page or types a URL into their browser's address bar, their browser — the **client** — communicates with a web **server** asking it to provide a resource (eg the content hosted at a particular URL). The server replies with a HTTP response, which, if successful, will include the requested resource.

A 'client' is commonly a web browser, but it may also be a mobile app or IoT device. The 'server' may be a web server, a database or email server.

Tag management systems can be run on the 'client-side' — where the user's browser is instructed to execute the tags. They can also be delivered by 'server-side' solutions — where event data received from the client-side is further processed and distributed to various tag partners on a remote server.

These tag partners may not be directly collecting the information from the user, rather they may be obtaining information from the party deploying the tag management system.

Regulation 6 applies in both a 'client-side' and 'server-side' context where information is stored or accessed on a device. Where personal data is involved, both the tag management deployer and other parties receiving the information have responsibilities under the UK GDPR.

The use of server-side tags may provide benefits to users, including faster page loading times. But it can also mean that the data being collected, and any third parties the data is shared with, may

not be visible to the user. For this reason, website operators using a server-side tag manager **must** inform the user about third parties it shares the information with.

Example

An e-commerce organisation uses a tag management system to centrally configure its JavaScript tags without needing to directly edit its website's code.

The tag management system allows the organisation to collect information from JavaScript tags to understand its users. This information includes:

- the device operating system, browser and version;
- screen dimensions of their device; and
- specific 'events' like whether they completed a purchase.

The organisation also integrates tags from:

- a third-party social media platform, to help the organisation to measure the effectiveness of their advertising campaigns;
- an adtech partner specialising in re-marketing campaigns; and
- an analytics platform that helps the organisation understand their user journeys.

The organisation's use of JavaScript tags for non-exempt purposes (eg advertising) requires consent under PECR. If the organisation uses them for exempt purposes (eg analytics in line with the statistical purposes exception) then it **must** ensure the user can object. This is the case regardless of whether the tag management system is running on the client-side or server-side.

What are the PECR rules?

At a glance

- You **must** tell users about any storage and access technologies you use and explain what they do. You **must** obtain prior consent to the UK GDPR standard for their use, unless an exception applies.
- The rules cover any use of storage and access technologies. They are not limited to particular environments or software (eg traditional ‘desktop’ websites and web browsers).
- The rules do not apply in the same way to intranets. However, wherever you collect personal data using storage and access technologies, including via an intranet, the requirements of data protection law still apply.
- These rules apply to any organisation running an online service, including public authorities.
- If you are a UK-based organisation but host your online service overseas, you **must** still comply with PECR.

In detail

- [What does PECR say about storage and access technologies?](#)
- [Who are subscribers and users?](#)
- [What is terminal equipment?](#)
- [What does ‘clear and comprehensive’ mean?](#)
- [What does ‘consent’ mean?](#)
- [Do the rules only apply to websites and web browsers?](#)
- [Do the rules apply to our internal network?](#)
- [Do the rules apply to public authorities?](#)
- [Do the rules apply to services based outside the UK?](#)
- [What if children are likely to access our service?](#)

What does PECR say about storage and access technologies?

Regulation 6 states:

“Subject to schedule A1, a person must not store information, or gain access to information stored, in the terminal equipment of a subscriber or user.”

Schedule A1 lists the exceptions to this rule, explained in the ‘[What are the exceptions?](#)’ section. This means that, unless an exception applies, if you use any storage and access technologies, you **must**:

- tell the subscriber or user what the technologies are;
- explain what they do; and
- obtain prior consent for their use.

[Relevant provisions in PECR – see regulation 6](#)

<https://www.legislation.gov.uk/uksi/2003/2426/regulation/6>

[Relevant provisions in PECR – see schedule A1](#)

<https://www.legislation.gov.uk/uksi/2003/2426/schedule/A1>

Who are subscribers and users?

These rules apply to the ‘terminal equipment’ of the ‘subscriber or user’.

The ‘subscriber’ is the person named on the bill for the supply of the service. For example, the telephone line or internet connection.

The ‘user’ is the person actually using the device to access the service.

In many cases the subscriber and the user may be the same. For example, someone that uses their computer or mobile device to access an online service over the broadband connection they pay for.

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 a service from their own device, they are a user.

What is terminal equipment?

‘Terminal equipment’ means someone’s device. The term is broad, and includes:

- desktop or mobile devices; and
- other connected devices (eg smart TVs, wearables, connected vehicles and other ‘internet of things’ (IoT) devices).

What does ‘clear and comprehensive information’ mean?

For most uses of storage and access technologies, PECR says you **must** provide ‘clear and comprehensive information’ about the purposes you want to use them for.

PECR does not define what ‘clear and comprehensive’ information means. However, in practice this refers to the UK GDPR’s transparency requirements, the right to be informed and the conditions for consent.

This means when you use storage and access technologies, you **must** provide the same kind of information to subscribers and users as you have to when you process their personal data. And in some cases, your use of the technologies will involve the processing of personal data anyway.

You **must** include the following information:

- what storage and access technologies you plan to use;
- the purposes you plan to use them for;
- whether any third parties either store or access information in the user’s device, or receive this information; and
- how long you intend to store or access information (eg the duration of any cookies you want to set).

These requirements apply to your use of any storage and access technologies, including those you incorporate from other organisations (eg online advertising networks or social media platforms).

Further reading - ICO guidance

[The right to be informed](#)

What does ‘consent’ mean?

Regulation 2(1) of PECR states that:

“ ‘consent’ by a user or subscriber corresponds to the data subject’s consent in the UK GDPR (as defined in section 3(10) of the Data Protection Act 2018).”

This means that, for PECR, the UK GDPR definition of consent applies.

The UK GDPR defines consent in Article 4(11) as:

“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.”

The UK GDPR also includes specific requirements for consent. It says that you **must**:

- be able to demonstrate you have valid consent;
- make your consent requests “clearly distinguishable from other matters” (ie you **must not** bundle them as part of terms and conditions, wherever possible);
- put your consent requests in an intelligible and easily accessible form, using clear and plain language;
- allow people to withdraw their consent at any time through your consent mechanism; and
- make it as easy for people to withdraw consent as it is for them to give it.

For storage and access technologies in PECR, this means that you **must**:

- ensure consent involves a clear and positive action from a subscriber or user. For example, continuing to use your website does not constitute valid consent, nor does the use of a pre-ticked box or equivalent;
- clearly inform subscribers or users about what storage and access technologies you want to use, what they do and what purposes you want to use them for before they consent;
- clearly and specifically name any third parties whose storage and access technologies you are asking subscribers or users to consent to. This includes when you are using storage and access technologies which may appear to be coming from the host domain, but are being used by a third party;
- **not** use any storage or access technologies for non-exempt purposes before the subscriber or user has given consent;
- enable subscribers or users to refuse the use of storage and access technologies for non-exempt purposes as easily as they can accept; and
- provide users with controls over any use of storage and access technologies for non-exempt purposes.

Do the rules only apply to websites and web browsers?

No. The rules cover any use of storage and access technologies. This means they are not limited to particular environments or software (eg traditional ‘desktop’ websites and web browsers).

For example, mobile apps commonly use embedded software development kits (SDKs) or other frameworks. These can be used for a range of purposes, such as app analytics tracking or

embedding functionality like logins or payment features. This involves storing information (or accessing information stored) on the device.

However you provide your online service (eg a website, a mobile app, or anything else), you are responsible for understanding the behaviour of any software components the service includes that may store information, or access information stored, on a user's device. This is particularly important if your service incorporates someone else's software component (eg third-party code).

The rules also apply when you collect or monitor information that terminal equipment automatically emits, such as wifi probe requests.

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 network, and therefore PECR do not apply in the same way. Similarly, PECR is unlikely to apply if you extend your private network to trusted third parties with access controls.

However, wherever you collect personal data using storage and access technologies, including via an intranet, the requirements of data protection law still apply.

Similarly, you **must** consider data protection requirements if you are using information from storage and access technologies for monitoring your workers, for example.

Further reading — ICO guidance

[Employment practices and data protection: monitoring workers](#)

Do the rules apply to public authorities?

Yes. These rules apply to any organisation running an online service, including public authorities.

Do the rules apply to services based outside the UK?

If you are a UK-based organisation but host your online service overseas, you **must** still comply with PECR. For example, if you use cloud services based in Europe or the USA.

PECR does not have specific rules about organisations who are based outside the UK and whose services are accessible in the UK. But, if those services process personal data then the UK GDPR may apply.

Online services with global availability won't automatically have to comply with the UK GDPR just because people in the UK can access them. However, you **must** comply with the UK GDPR if you are processing data that:

- relates to the offer of goods or services to people in the UK; or
- monitors the behaviour of people in the UK.

If you don't tell people about how you use storage and access technologies to process their personal data, your processing won't be fair, lawful or transparent.

If you are based overseas but don't offer goods or services in the UK or monitor the behaviour of people in the UK, then you **could** implement appropriate technical and organisational measures to demonstrate this. For example by:

- making clear and accurate statements to this effect on the service (eg in the privacy information or similar);
- not using any storage and access technologies to monitor UK user behaviour; or
- preventing users from accessing your service (eg via IP address blocking).

However, implementing any of the above measures does not automatically mean that your organisation is out of scope of the UK GDPR. Rather, it depends on your organisation's specific circumstances.

Example

An online news outlet based outside the UK, but accessible to people within the UK, may not be in scope of the UK GDPR, depending on its circumstances.

The outlet may carry news reports relating to the UK, but if this content is directed at people within the outlet's own country or territory, rather than people in the UK, it is not in scope of the UK GDPR, even if those people 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 people in the UK. In this instance, it **must** consider whether the UK GDPR's territorial provisions apply to it.

Example

The same online news outlet uses cookies for behavioural advertising purposes, where it processes information about all visitors to its service to create profiles about them. It uses these to target adverts based on actual or inferred interests and behaviours.

The use of cookies for these purposes would result in the storage and access of information in the devices of all visitors to the website, regardless of their location. For visitors in the UK, this processing may constitute monitoring the behaviour of people in the UK and is therefore in scope of the UK GDPR. The news outlet **must** ensure its use of personal data complies with the law (eg by obtaining valid consent).

Further reading — ICO guidance

[Receiving personal information from the EEA](#)

What if children are likely to access our online service?

PECR does not have specific provisions about children accessing your online service.

If you are processing children's data, then you **must** ensure you are complying with the UK GDPR.

If your online service is likely to be accessed by a child, then you **should** conform with our Children's code.

Further reading — ICO guidance

- [The Children's Code Hub](#)
- [Children's information](#)

What are the exceptions?

At a glance

- There are five exceptions to the prohibition on storing or accessing information on people's devices.
- The exceptions only apply if your use of storage and access technologies aligns with the purposes and requirements of each one. If your usage goes beyond these, you **must** get consent.
- The 'communication' exception only applies when the sole purpose of the storage or access is for the transmission of a communication.
- The 'strictly necessary' exception applies when the purpose of the storage or access is essential to provide the service the subscriber or user requests.
- The 'statistical purposes' exception applies when the sole purpose of the storage or access is so you can collect information for statistical purposes about the use of your service.
- The 'appearance' exception applies when the purpose of the storage or access is to adapt the way your service appears or functions in line with the subscriber's or user's preference.
- The 'emergency assistance' exception applies when the sole purpose of the storage or access is to identify the geographical position of the subscriber's or user's device to provide emergency assistance.
- The statistical purposes and appearance exceptions say that you **must** provide subscribers and users with 'a simple means of objecting, free of charge, to the storage or access'.

In detail

- [Do all storage and access technologies require consent?](#)
- [What is the 'communication' exception?](#)
- [What is the 'strictly necessary' exception?](#)
- [What is the 'statistical purposes' exception?](#)
- [What is the 'appearance' exception?](#)
- [What is the 'emergency assistance' exception?](#)
- [What does 'a simple means of objecting' mean?](#)

Do all storage and access technologies require consent?

No. You can store or access information in five circumstances without the subscriber's or user's consent. These exceptions apply when storage or access is:

- for the sole purpose of the transmission of a communication. This is the 'communication' exception;

- strictly necessary to provide the service the subscriber or user requests. This is the ‘strictly necessary’ exception;
- for the sole purpose of collecting statistical information about visitors to your service, with a view to improving it. This is the ‘statistical purposes’ exception (also known as the ‘analytics’ exception);
- for the sole purpose of improving or adapting the appearance or functionality of the service to the subscriber’s or user’s preference. This is the ‘appearance’ exception; or
- for the sole purpose of identifying the location of a subscriber or user who requires emergency assistance. This is the ‘emergency assistance’ exception.

An exception means that the purpose for which you want to store or access is exempt from the prohibition. With the ‘statistical purposes’ and ‘appearance’ exceptions, you **must** give subscribers or users:

- clear and comprehensive information about your use of the technology; and
- an easy way to object to this use.

If you don’t, you won’t be using those exceptions correctly. This means you **must not** use the technology without the subscriber’s or user’s consent.

The following sections explain each exception in detail, along with the specific requirements for each one. When assessing whether any of the exceptions apply, you **must** consider their specific requirements. This is because exceptions are narrow in scope and won’t apply in all cases.

Relevant provisions in PECR - see regulation 6

<https://www.legislation.gov.uk/uksi/2003/2426/regulation/6>

Relevant provisions in PECR - see schedule A1

<https://www.legislation.gov.uk/uksi/2003/2426/schedule/A1>

Further reading

[How should we obtain, record and manage consent?](#)

What is the ‘communication’ exception?

The communication exception is about the transmission of a communication over an electronic communications network.

Three elements are necessary for a communication to take place over a network between two parties. These are the ability to:

- route information over a network by identifying the communication ‘endpoints’ — devices that accept communications across that network;
- exchange data items in their intended order; and
- detect transmission errors or data loss.

The communication exception covers the use of storage and access technologies that fulfil one (or more) of these properties, but only for the sole purpose of the transmission.

For this exception to apply, you **must** ensure that the transmission of the communication is impossible without the use of the particular storage and access technology.

Common examples include:

Activity	Likely to meet the communication exception?
Session cookies for load balancing purposes, with the sole purpose of identifying which server in the pool the communication will be directed to.	✓
Device fingerprinting techniques, solely for network management purposes.	✓

What is the ‘strictly necessary’ exception?

The ‘strictly necessary’ exception applies when the purpose of the storage or access is **essential** to provide the service the subscriber or user requests.

This means that without it the service couldn’t be provided on a technical level.

Importantly, the exception only applies to ‘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 the service is an ISS.

The exception also covers the use of storage and access technologies to comply with any other legislation that applies to you (eg the security requirements of data protection law).

However, this exception will only apply if the technology is the only reasonable and proportionate way to comply with the requirements of the other legislation. It does not apply if there are ways to comply with this other legislation without the use of storage and access technologies or without the specific technologies you are choosing to use.

The strictly necessary exception is about what’s essential to deliver a service that the user requests. So, whether storage or access is ‘strictly necessary’ inherently depends on the user’s

perspective – without it, you cannot provide the requested service. This means that you **should** assess ‘strictly necessary’ from the point of view of the subscriber or user, not your own.

For example, you might view the use of advertising cookies as ‘strictly necessary’ because they bring in revenue that funds your service. However, they are not ‘strictly necessary’ from the user’s perspective. There are no advertising purposes that meet the strictly necessary exception.

What activities are likely to meet this exception?

PECR gives some non-exhaustive examples of activities that meet this exception:

- ensuring the security of terminal equipment;
- preventing or detecting fraud;
- preventing or detecting technical faults;
- authenticating the subscriber or user; and
- recording information or selections the user makes on an online service.

Some of these examples may apply to you, depending on how your online service functions.

The table below includes non-exhaustive examples of activities that are likely to meet the exception, and those that won’t.

Activity	Likely to meet the strictly necessary exception?
Remembering the goods a user wishes to buy when they go to the online checkout or add goods to their shopping basket.	✓
Complying with the security requirements of data protection law for an activity the user has requested (eg, in connection with online banking services).	✓
Identifying a user once they have logged in to an online service for the duration of their visit to the site (eg to prevent a new login prompt on an online banking service each time the user loads a new page).	✓
Using link decoration to authenticate a user.	✓
Session cookies used to store a user's preference can rely on the strictly necessary exception, provided they are not linked to a persistent identifier. The exception 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	✓

<p>sufficient for consent to be obtained for any cookies relating to that mechanism, provided the user is given clear and comprehensive information that a persistent cookie will be set on their device for the purpose of remembering their consent preference.</p> <p>However, the information accessed must be used solely for this purpose. Any secondary purposes mean the exception would not apply.</p>	
<p>Streaming content:</p> <p>The use of storage and access technologies to provide streaming content can be exempt in some circumstances.</p> <p>For example, if your service is an online content provider, then you can rely on the exception for purposes that relate to the technical provision of the content.</p> <p>This is because accessing the video or audio is part of the service the user has requested.</p> <p>This can also apply in circumstances where you are providing content to the same user on different devices. For example, if a user pauses their stream on their connected TV and later resumes that stream on their mobile device, they would expect the service to resume from where they had paused the stream.</p> <p>However, the exception does not extend to other purposes, such as content personalisation or usage monitoring.</p>	<p>✓ (in some circumstances).</p>
<p>Hosting embedded content:</p> <p>If your service includes content hosted on these platforms (eg if you have posted a video on your organisation’s YouTube channel), you should:</p> <ul style="list-style-type: none"> • configure the embedded content not to set storage and access technologies the instant someone visits the page with it on, including for analytics purposes; and • tell the user underneath the embed that if they choose to press ‘play’, storage and access technologies will be used (you should use a ‘privacy mode’ where available). This will not require consent, as the user has been informed and wants to access the content. <p>When considering how to manage your use of embedded videos, you could:</p> <ul style="list-style-type: none"> • add a consent request into your existing mechanism; or • use a ‘just-in-time’ approach to seek consent on particular pages where the videos are included. <p>Alternatively, you could consider using external links instead of embedded videos.</p> <p>Adding a consent request for embedded videos into your consent mechanism may seem like the simplest option. However, if you do this,</p>	<p>✓ (in some circumstances).</p>

<p>you must provide clear and comprehensive information to your users about what this means for them. For example, by saying that:</p> <ul style="list-style-type: none"> • if they enable the storage and access technologies, this may result in the video sharing platform collecting information about their viewing (eg for analytics and advertising purposes); and • if they don't enable the storage and access technologies, they will see external links to the videos instead. <p>You should configure your use of these external services in the most privacy-friendly way possible. What this involves depends on the controls and functions available on your service.</p>	
<p>Cashback and rewards services:</p> <p>When someone signs up to an online service offering cashback or rewards, it is likely that some storage and access technologies set by that service would be essential as the user has requested that service.</p> <p>However, storage and access technologies that may be strictly necessary to provide one service are not automatically strictly necessary to provide another, different service. Equally, you must limit the use of the storage and access technology to the purpose that is necessary to provide the service.</p> <p>When deciding if storage and access technologies delivered on a service for rewards or cashback purposes meet the 'strictly necessary' exception, you should consider:</p> <ul style="list-style-type: none"> • how that service operates, including what cookies are set, by whom and in what circumstances; • the different ways in which users can engage with that service; • the arrangements the service may have with other parties (eg merchant, retail or advertising partners); and • the processing operations of any storage and access technologies they use. <p>Where your service partners with another service, you must work together to determine your respective compliance obligations.</p>	<p>✓ (in some circumstances).</p>
<p>Social media plugins and tracking technologies:</p> <p>If you decide to use social media plugins or other tracking technologies on your service, you must be aware of what these technologies do and how they work.</p> <p>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.</p> <p>In such cases, the storage and access of information by these plugins can</p>	<p>X</p>

<p>be strictly necessary for the functionality the user has requested on your service.</p> <p>However, this does not apply to non-logged in users of that social media platform — whether these are users who have logged out, or users that are not members of that network.</p> <p>So, you must get consent for any use of social plugins, unless you configure them to only store or access information on devices that logged-in members of the social media platform use.</p> <p>Where a social media plugin, script, cookie or other technology tracks users, the exception does not apply.</p> <p>Therefore, you must obtain consent for the use of social media tracking technologies you include in your online service. This applies whether or not your users are members of the social network in question.</p>	
<p>Cross-site or cross-device tracking:</p> <p>You must get consent for any cross-site or cross-device tracking you want to do. The use of storage and access technologies to link a particular user across sites and devices is not strictly necessary to provide your service.</p>	X
<p>Online advertising:</p> <p>If your service uses storage or access technologies for the purposes of online advertising, you must get consent. You cannot rely on any of the exceptions. Online advertising purposes are not exempt from PECR's consent requirements and never have been.</p> <p>This includes any advertising-related purpose, including (but not limited to) things such as frequency capping, ad affiliation, ad measurement and performance, click fraud detection, market research, product improvement or debugging.</p> <p>You must also get consent if you are using device fingerprinting techniques for online advertising purposes. 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.</p>	X

Also, if you say your use of a particular technology is strictly necessary because of the purpose (eg security), you **must** ensure that you only use it for this purpose. If you use it for any other purpose as well, the exception does not apply and you **must** then get consent.

Further reading - ICO guidance

- [Age appropriate design](#) - see ‘What do you mean by an information society service?’
- [Profiling tools for online safety](#) - see ‘How does PECR apply to profiling tools?’

What is the ‘statistical purposes’ exception?

The statistical purposes exception means you don’t have to get consent for storing or accessing information on a device if:

“the sole purpose of the storage or access is to enable the person -

(i) to collect information for statistical purposes about how the service is used with a view to making improvements to the service, or

(ii) to collect information for statistical purposes about how a website by means of which the service is provided is used with a view to making improvements to the website.”

This exception applies when:

- you are an ISS provider; and
- the sole purpose of the storage and access technology is collecting information for statistical purposes about the use of your service.

You can share this information with a third party, provided they are only using it to improve your website or service.

As part of relying on this exception, you must provide the user or subscriber with clear and comprehensive information about the purpose, and a ‘simple and free’ means to object.

The statistical purposes exception does not apply to collecting or monitoring information automatically emitted by terminal equipment, such as wifi probe requests.

What activities are likely to meet the exception?

The exception is about:

- the creation of aggregate statistical information about visitors to your service; and
- your use of this information for the purpose of improving it.

The exception is essentially for analytics purposes. However, it is not a broad exception that covers all types of analytics technologies or ways you can use them. It is about how your service is used, not about who uses it. It is not for identifying, tracking or monitoring people or groups of people who use your service. It also doesn’t apply to things like online advertising.

To rely on it, you **must** ensure your analytics involve statistical information. For example, things like:

- how many people access your service;
- what they access; and
- how long they access it for.

‘Improving the service’ includes things like understanding user journeys through your website, and which areas of your website your visitors spend most or least time on. For example, to decide how to organise your online service, what content to produce more or less of, or to improve your users’ experience.

Statistical purposes is not defined in PECR itself, but in practice it can be taken to mean the same as defined in the UK GDPR, for information, not just personal data:

“References in this Regulation to the processing of personal data for statistical purposes are references to processing for statistical surveys or for the production of statistical results where—

(a) the information that results from the processing is aggregate data that is not personal data, and

(b) the controller does not use the personal data processed, or the information that results from the processing, in support of measures or decisions with respect to a particular data subject to whom the personal data relates.”

It’s likely this processing involves collecting individual-level information for this purpose. This may be personal data (eg where it relates to a specific visitor of the service). If that is the case, you **must** also comply with the UK GDPR.

You **must** also then aggregate this information. You **must** ensure that you do not store any personal data for any longer than is necessary for your aggregation process.

If your processing goes beyond this, the exception won’t apply and you **must** get consent. For example, if you:

- make inferences or take decisions about people (or categories of people) based on information like their IP address or category on your service; or
- retain the individual-level information (after aggregating it).

The statistical purposes exception enables you to understand how visitors interact with your service. Provided your use of storage and access technologies for this purpose is in line with the exception, you don’t need to get consent under PECR.

To rely on the exception, you **must** only use the storage and access technologies for the purpose of improving your service or website, and not for any other purposes. This is the case whether you store or access information for this purpose, or whether you use a third party, such as an analytics provider to do this for you. You **must** ensure that the information resulting from the storage or access is aggregate statistical information that you cannot use to identify people.

The table below includes non-exhaustive examples of activities that are likely to meet the exception, and those that won't.

Activity – when using aggregate statistical information	Likely to meet the statistical purposes exception?
Total visits to your website, page-by-page (eg for traffic analysis to understand user journeys).	✓
User interactions with pages on your website (eg average scroll depth or the total number of hits on sections of a page).	✓
Information to understand how your users access your service (eg device types and browser or operating system versions).	✓
How your users reached your service. For example, via an email campaign (ie the referrer URL), search results or anything else.	✓
A/B testing - separating users into two groups to compare user interactions with two different versions of your website or particular sections of it.	✓
Coarse geolocation information of website users (eg at city or region level) that does not allow people to be identified.	✓
Information on page loading speeds, bounce rates or exit pages (eg to detect browsing issues).	✓
<p>Using web analytics tools to monitor or track people: The statistical purposes exception does not allow you to monitor or track individual visitors to your service. You must obtain consent for:</p> <ul style="list-style-type: none"> • logs or recordings of individual visitors to your website and the actions they took (if not obtained for the purposes of security); • information on whether users viewed or clicked on an advert displayed to them, for the purpose of measuring the performance of the advert; • connecting a visitor ID to their site activity (eg where users purchased a product on your website ('conversions') to be shared with advertising partners); • tracking or profiling individual visitors or categories of visitors 	X

(eg based on their IP address or the pages they visited on your website); or	
<ul style="list-style-type: none"> • monitoring the browsing of website visitors across different services and applications. 	
<p>Online advertising:</p> <p>The statistical purposes exception does not apply to purposes related to online advertising. For any use of storage and access technologies for these purposes, you must get consent.</p>	X

Neither PECR nor the UK GDPR specifies any timeframes for aggregating your information. You **should** therefore determine the appropriate timeframe for your service based on its particular circumstances, including your visitor numbers. You **could** consider daily aggregation to be appropriate for your service. A more frequent aggregation (such as hourly) of some data points may be appropriate in some cases (eg if you have a large number of visitors).

You **must** only store individual-level information for as long as you need it, regardless of your aggregation frequency.

You **must** implement appropriate technical and organisational measures to ensure that your aggregated datasets don't allow people to be identified.

Where analytics involves personal data, you **must** consider the UK GDPR requirement for 'data protection by design and by default'. This includes when you are considering making use of a third-party provider.

Further reading – ICO guidance

- [Anonymisation](#)
- [Privacy-enhancing technologies \(PETs\)](#)

Can we use a third-party analytics service?

Yes. The exception recognises that you can:

- develop your own analytics solution; or
- use a third-party analytics provider.

Paragraph 5(1)(c) of schedule A1 states:

“Any information that the storage or access enables the person to collect is not shared with any other person except for the purpose of enabling that other person to assist with making improvements to the service or website.”

This means, for the statistical purposes exception to apply, you **must** ensure that the third party only assists you in achieving your purpose. Your provider can only:

- act on your behalf; and
- use the information to help **you** improve **your** service.

Whether you choose to use a third-party analytics provider is a decision for you to take, based on your circumstances.

If you do use a third-party provider, you **must**:

- tell your users that you do so; and
- explain what the third party does with the information it collects.

Where you are using a third party analytics provider, you **must** also consider your UK GDPR obligations.

This means that you **must**:

- clarify the roles and responsibilities between you and your analytics provider. (To rely on the exception, your third party provider **must** be a processor, not a joint controller);
 - specify what the provider will do on your behalf;
 - ensure the provider only uses the information to improve your service and does not link it with other information from any other information it works with; and
 - consider your obligations if the processing involves international transfers of personal data.
-
- obtain consent, if you use a third party service for other purposes. For example to link a user’s activity and purchase journey on your website to an online advert they may have previously clicked on.

Example

A website operator posts articles on different topics. The operator wants to understand which of its articles visitors read deeply, and which ones they don’t have the same level of interest in. It wants to use this to inform what type of content to produce in future.

The operator decides to use a third-party analytics service for this purpose. The analytics service provides JavaScript that the operator adds to relevant pages. This measures scroll depth, time spent on each page, and the bounce rate.

The operator accesses this information by logging into its account at the analytics service. They can see the statistics about the average time visitors spend on particular pages and how much they read.

The operator can rely on the statistical purposes exception in these circumstances.

Example

The same website operator now wants to understand the characteristics of those visitors that read articles most deeply. Working with the analytics service, the operator chooses additional parameters to incorporate into the analytics technology on its website. These parameters process additional information in order to segment visitors by demographic, including age group and gender.

The operator intends to use this information to determine what content to promote to these particular visitors in future.

For this storage and access, the operator cannot rely on the statistical purposes exception. This is because what it wants to do goes beyond the exception's scope by including profiling to target content.

Further reading – ICO guidance

- [Controllers, joint controllers and processors](#)
- [Contracts](#)
- [A guide to international transfers](#)
- [Data protection by design and by default](#)

What is the 'appearance' exception?

The 'appearance' exception applies when the sole purpose of the storage and access is so you can either:

- adapt the way your service appears or functions in line with the subscriber's or user's preference; or
- otherwise enhance the appearance or functionality of the website when displayed on, or accessed by, the subscriber's or user's device.

To rely on this exception, you **must** also provide the subscriber or user with clear and comprehensive information about the purpose, and a ‘simple and free’ means to object.

This exception is not about adapting the content to display to a user on your service based on known or inferred interests or behaviours about them. For example, using their profile or previous browsing history to decide what content to promote at the top of the webpage, or to choose which advert to serve.

These purposes do not meet the exception and you **must** obtain consent.

You **must** also ensure that you limit any processing of personal data related to the use of storage and access technologies for purposes under this exception to what is necessary for this purpose.

The table below includes non-exhaustive examples of activities that are likely to meet the exception, and those that won’t.

Activity	Likely to meet the appearance exception?
Identifying the dimensions of a subscriber’s or user’s monitor or screen to enable reconfiguration of a webpage to adapt to the screen (‘responsive design’). For example, to display a simplified navigation and layout to a user visiting your website from a mobile device.	✓
Remembering the language the subscriber or user selects (eg on a multilingual website).	✓
<p>The use of an external font library to display your chosen font on the service: You should ensure the font provider uses this information for the purposes of serving the font that you’ve selected and not for other purposes (eg advertising and profiling).</p> <p>Be aware that external font libraries may collect information about your users, such as their IP address. Where this occurs, you must explain this to your users and give them a simple and free way to object.</p> <p>You could consider self-hosting fonts by downloading them from an external service and uploading them to your server.</p>	✓
<p>Detecting preferences indicated on the subscriber’s or user’s operating system, such as themes and colour schemes, and displaying the service using a similar theme, if available.</p> <p>For example, a user might turn on ‘dark mode’ in their mobile device settings. A video player app can use this preference to display its app features in its own dark mode setting. The user can easily switch away from dark mode within the app.</p>	✓

Using device information to optimise user experience on your service (eg device memory information to tailor the features to display to that user). You must not use this information for other purposes beyond what is required to improve the appearance or functionality of the service (eg device fingerprinting techniques to identify a user).	✓
Changing the content you display to a user on your service based on known or inferred interests or behaviours about them. For example, using their profile or previous browsing history to decide what content to promote at the top of the webpage, or to choose which advert to serve. Any purposes relating to decisions about the content on your service do not meet this exception and you must get consent.	X
Online advertising: The appearance exception does not apply to purposes related to online advertising. For any use of storage and access technologies for these purposes, you must get consent.	X

What is the ‘emergency assistance’ exception?

This exception applies where the sole purpose of the storage or access is to identify the geographical position of the subscriber’s or user’s device to provide emergency assistance.

It’s similar to the emergency calls exception in regulation 16 of PECR, which allows the restrictions on the processing of location data to be removed when the user makes an emergency call.

The difference is that the information stored or accessed isn’t limited to location data as defined by PECR, nor is it limited to emergency calls. Specifically, it allows you to use information about someone’s location for emergency assistance purposes. This includes using GPS-based location information from smartphones, tablets, sat-navs or other devices. This information isn’t covered by PECR definition of location data, as they are not collected by a network or service.

This means that the emergency assistance exception allows you to process more information for the purposes of providing this assistance to the subscriber or user.

For the exception to apply, you **must**:

- receive a communication from the subscriber or user seeking emergency assistance first; or
- receive another indication that the subscriber or user needs emergency assistance.

In practice, this exception only applies in limited circumstances, including those listed in the table below.

Activity	Likely to meet the ‘emergency assistance’ exception?
Motor vehicle ‘eCall’ functionalities that automatically contact emergency services on behalf of the subscriber or user, as the subscriber or user would	✓

have enabled this feature before the incident.	
Personal safety alarms that use GPS features to send location information once the subscriber or user wearing them presses an emergency button.	✓
Smart watches with fall detection or pulse detection functionality. When the user or subscriber has enabled this feature, the watch can call the emergency services when a fall or lack of pulse is detected without them initiating it, once an opportunity for the user to cancel the call has expired.	✓

Relevant provisions in PECR - see regulations 2, 14(2), 16
<https://www.legislation.gov.uk/uksi/2003/2426/contents/made>

Further reading

[Guide to PECR – Location data](#)

What does ‘a simple means of objecting’ mean?

The statistical purposes and appearance exceptions say that you **must** provide subscribers and users with:

'a simple means of objecting, free of charge, to the storage or access'

Part of relying on these exceptions is providing the ability for subscribers and users to object. If you don't offer this, what you're doing isn't in line with either exception.

PECR does not define what this ‘simple means of objecting’ looks like. You **could** provide it through your existing consent mechanism. For example, by having your ‘statistical purposes’ or ‘appearance’ toggles on by default, with the ability for users to change them to off at any time. See ‘[Our expectations for consent mechanisms](#)’ for a visual example of what this may look like in practice.

It's also the case that these two exceptions only apply where:

‘the subscriber or user [...] does not object’

This means that if someone does object, you **must** stop storing or accessing information on their device. But if the user indicates that they have changed their mind later (eg by toggling the purpose back to on), then you can store or access information again by relying on the particular exception.

Similar to [consent](#), some subscribers and users might exercise their choices through things like their browser settings. But this won't always be the case. You **must not** solely rely on browser settings as an indication of whether a person does not object. You can't assume that each visitor to your online service has either configured their browser in this way or that their browser even has these features.

How do the PECR rules relate to the UK GDPR?

At a glance

- If you are using storage and access technologies, you **must** consider PECR compliance before you look to the UK GDPR.
- If you have to obtain consent for your use of storage and access technologies, and the information is personal data, then you **should** use consent as your lawful basis under the UK GDPR for subsequent processing.
- If your use of the storage and access technologies does meet an exception and the information is personal data, any of the lawful bases in the UK GDPR may apply, depending on your specific circumstances.
- You **must not** retrospectively use the legitimate interests lawful basis to justify processing in cases where you encounter problems with the validity of consent.

In detail

- [What is the relationship between PECR and the UK GDPR?](#)
- [What does the UK GDPR say about storage and access technologies?](#)
- [How does PECR consent fit with the fit lawful basis requirements of the UK GDPR?](#)
- [What does PECR say about subsequent processing?](#)

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 about privacy and electronic communications. Where these rules apply, they take precedence over the DPA and the UK GDPR. This means that when you are using storage and access technologies, you **must** consider PECR compliance before you look to the UK GDPR.

Additionally, PECR depends on data protection law for some of its definitions. For example, PECR takes the UK GDPR's standard of consent.

If you operate an online service, then the easiest way to look at the two laws is:

- if you store information, or access information stored, on user devices, then you **must** comply with PECR first; and
- the UK GDPR applies to any processing of personal data outside this storage or access.

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

‘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 processing personal data generally have greater privacy and security implications.

Where the use of storage and access technologies does involve processing personal data, you **must** ensure you comply with the additional requirements of the UK GDPR.

[Relevant provisions in PECR - see regulation 4](https://www.legislation.gov.uk/uksi/2003/2426/regulation/4)

<https://www.legislation.gov.uk/uksi/2003/2426/regulation/4>

What does the UK GDPR say about storage and access technologies?

It is important to note that regulation 6 of PECR is about ‘information’, not ‘personal data’. This means the rules apply whether or not your use of storage and access technologies involves processing personal data.

The UK GDPR doesn’t specifically refer to storage and access technologies in the way that PECR does. This is because PECR contains specific rules on their use. However, it:

- includes ‘online identifiers’ in the definition of personal data; and
- refers to cookies and IP addresses as types of these identifiers.

This means that where information like an online identifier relates to a person, it is personal data. For example, a user authentication cookie is a type of online identifier that involves processing of personal data, as it is used to enable someone to log in to their account with an online service provider.

Alongside cookies and IP addresses, online identifiers can include (but are not limited to):

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

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

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

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

While 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 and 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, you **must** ensure that your processing complies with the UK GDPR.

You **must** inform people about what information you are collecting, as well as how and for what purpose, if you collect information that either:

- builds up a picture about a person, allowing them to be identified; or
- may be combined alongside other data to identify a person at a later date.

You **must** inform people about what information is being collected, as well as how and for what purpose.

Further reading — ICO guidance

- [What is personal data?](#)
- [The right to be informed](#)

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

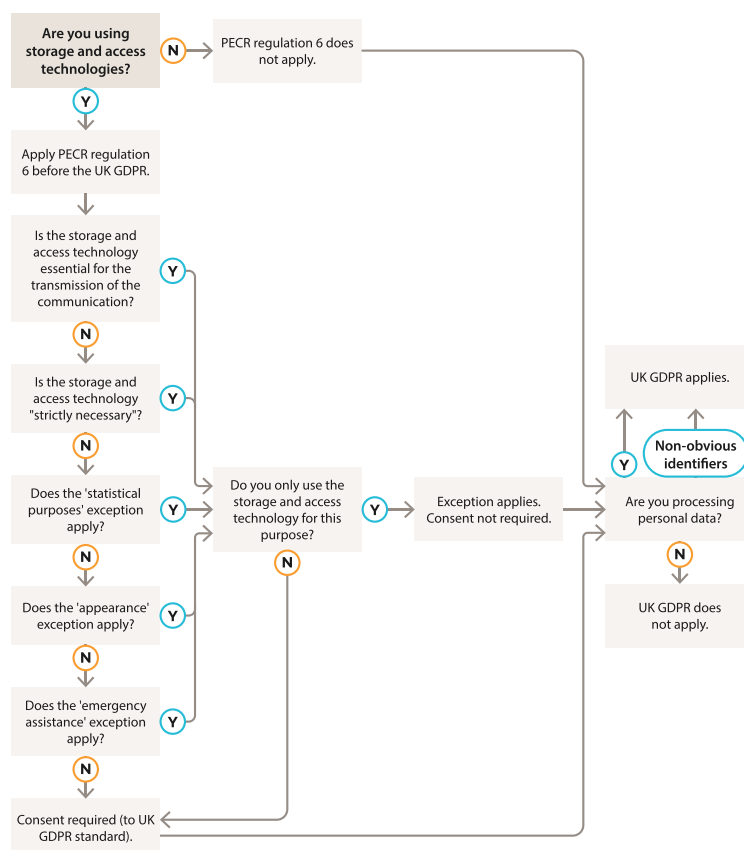
The UK GDPR has seven lawful bases for processing personal data. One of these is consent. No lawful basis is more important than any other. The most appropriate one depends on the specifics of your processing activities.

However, regulation 6 of PECR prohibits the storage and access of information on a device unless an exception applies or you obtain consent.

This means if regulation 6 applies, the full range of lawful bases under the UK GDPR are not always available to you.

If your use of the storage and access technologies does meet an exception and the information is personal data, any of the lawful bases in the UK GDPR may apply, depending on your specific circumstances.

You can use this flowchart to understand where the consent requirements apply for storage and access technologies.



[A text description of this flowchart is available.](#)

What does PECR say about subsequent processing?

Regulation 6 is specifically about the processing involved in storing information, or accessing information stored, in user devices. It does not apply to, or contain any specific rule about, subsequent processing operations involving this information.

If you rely on an exception for your use of storage and access technologies, but then the information you store or access is personal data, in principle any of the lawful bases may apply. You **must** determine the most appropriate one for your circumstances.

Example

An emergency service organisation is using the emergency assistance exception to store or access information (or both) on a user's device after receiving a communication that they need emergency assistance.

Location information is personal data under the UK GDPR, so the organisation needs a lawful basis to process this data.

Given it is an emergency situation, the organisation uses the vital interests lawful basis to process the user's personal data.

However, if you have to obtain consent for your use of storage and access technologies, and the information is personal data, then you **should** use consent as your lawful basis under the UK GDPR for subsequent processing. You can rely on this consent for the subsequent processing provided the consent sought under PECR was appropriate for the subsequent processing purpose(s).

Trying to apply another lawful basis such as legitimate interests is entirely unnecessary. It may also render your original consent request invalid. This is because it is likely the original consent will not have been freely given, informed, specific and unambiguous.

There may also be an element of unfairness as well. For example, in cases where people understand their personal data is processed on the basis of consent, yet once they withdraw consent, you continue to process via legitimate interests.

Also, seeking to rely on legitimate interests creates more work for you. Legitimate interests means that you take on extra responsibility for ensuring that people's interests, rights and freedoms are fully considered and protected.

You **must not** retrospectively use the legitimate interests lawful basis to justify processing in cases where you encounter problems with the validity of consent. This is because the use of storage and access technologies for non-exempt purposes requires consent in order to be lawful.

Further reading — ICO guidance

[A guide to lawful basis](#)

How do we comply with the PECR rules?

At a glance

- You **must** consider storage or access technologies as part of the design and implementation of your service and business practices.
- You **must** have appropriate arrangements in place with any third parties you are using to provide your service.
- In general, you **must** provide clear and comprehensive information about the storage and access technologies you use.
- PECR has some exceptions that mean you don't have to provide this in certain cases. But if your storage and access involves processing personal data, you **must** provide it anyway.
- You **must** explain your storage and access technologies in a way that anyone visiting your service can understand.
- You **must** not pre-enable non-exempt storage and access technologies.
- PECR does not specify how long you can use any storage and access technologies for. You **should** consider the appropriate duration in relation to the circumstances of your online service and for the purpose for which you want to use the technology.
- You **should** undertake regular reviews of your online service, as well as any storage and access technologies it includes.

In detail

- [Who is responsible for compliance?](#)
- [How do we consider PECR when designing a new online service?](#)
- [What do we need to consider if we use someone else's technologies on our online service?](#)
- [How do we tell people about the storage and access technologies we use?](#)
- [How do we tell people about storage and access technologies set on websites that we link to?](#)
- [Can we pre-enable any non-exempt storage and access technologies?](#)
- [How long can we store or access information for?](#)
- [What is an audit and how can we do one?](#)

Who is responsible for compliance?

PECR says that 'a person' **must not** store, or gain access to information stored, on a subscriber's or user's equipment, unless clear and comprehensive information is provided and consent is obtained.

In most cases, this means that as the service provider, you have the primary responsibility for compliance with PECR. For example, you are the person that makes decisions about:

- what the service is;
- what functions the service will have; and
- what storage and access technologies to use (and for what purposes), including whether your service incorporates third-party features or if you enable third-party storage and access technologies.

How do we consider PECR when designing a new online service?

If you are planning a new online service, you **must** put appropriate technical and organisational measures in place to implement data protection principles and safeguard individual rights, from the design stage right through the lifecycle of your service.

Under PECR, you **must** consider storage or access technologies as part of the design and implementation of your service and business practices. This includes:

- what storage and access technologies you want to use;
- which ones meet an exception (and why); and
- which ones require consent.

If you use third parties in the provision of your service, you **must** have appropriate arrangements in place. For example, if you plan to share any information with them or will have their features embedded in your website or service.

Following a data protection by design and by default approach is particularly important if you intend to provide your service via a mobile app. This is because:

- mobile devices such as smartphones and tablets are likely to have direct access to different sensors and data. For example, the microphone, camera and GPS receiver or wide-ranging information like the user's email accounts and contacts;
- users are likely to have a range of apps downloaded on their device for many different functions, which can involve sharing personal data (including sensitive data). For example, medical or fitness apps, social media apps and banking;
- app developers often make use of third-party SDKs for different purposes. These can introduce new and complex flows of information from the user's device when using the app, including use by third parties, which may not be obvious from the user interface; and
- mobile devices often have small screens, typically with touch-based interfaces. This can make it more challenging for apps to effectively communicate privacy information with app users (and obtain consent where required).

Similar considerations apply to connected IoT devices. Our guidance on consumer IoT contains further detail on how to take a data protection by design and by default approach to designing these products and services.

Further reading — ICO guidance

- [Data protection by design and by default](#)
- [Guidance on consumer IoT products and services](#)

What do we need to consider if we use someone else's technologies on our online service?

Other organisations provide a range of storage and access technologies. Your organisation might decide to deploy these on your service rather than trying to develop your own to, for example:

- provide a specific element, function or feature to your service (eg streaming content);
- secure your service and protect your users (eg security and authentication);
- help you generate revenue (eg through advertising technology); or
- enable your users to interact with other services or platforms (eg social media).

As the online service provider, it is your responsibility to understand the technologies you intend to use and ensure you comply with PECR.

Where your use of these technologies involves the processing of personal data, you **must** also consider the UK GDPR. For example by:

- being clear about which other organisations may be involved in the processing;
- allocating appropriate roles and responsibilities between you and these organisations (eg controllers, processors or joint controllers);
- identifying and mitigate risks to people's rights and freedoms; and
- ensuring that mechanisms are in place to facilitate individual rights between all parties involved and appropriate actions are taken (eg informing another organisation relying on consent you obtained from a user that they have since withdrawn that consent).

Depending on the circumstances, these other organisations may have their own responsibilities under the UK GDPR. Our data sharing code contains further information on their responsibilities.

Further reading — ICO guidance

- [Accountability and governance](#)
- [Controllers and processors](#)
- [Data sharing](#)
- [Data sharing: a code of practice](#)
- [Individual rights — guidance and resources](#)

How do we tell people about the storage and access technologies we use?

In general, you **must** provide clear and comprehensive information about the storage and access technologies you use.

PECR has some exceptions that mean you don't have to provide this in certain cases. But if your storage and access involves processing personal data, you **must** provide it anyway.

You **must** cover the following information:

- the storage and access technologies you intend to use;
- the purposes you intend to use them for;
- any third parties who store or access information in the user's device, or process information stored in, or accessed from, the user's device, including the purposes they will be used for; and
- the duration for which any information will be stored for, or access to information granted for, such as the duration of cookies.

Providing this is part of fulfilling your transparency requirements under data protection law.

These transparency requirements apply whenever you are processing personal data, even if you are making use of a PECR exception that does not require provision of clear and comprehensive information (eg the 'strictly necessary' exception).

You **must also** explain your storage and access technologies in a way that anyone visiting your service can understand. In particular, you **must** make the information:

- concise;
- transparent;
- intelligible;
- easily accessible; and
- in clear and plain language.

You **should** provide this information in as user-friendly way as possible.

You **must**:

- tailor the language to your audience;
- avoid complex or lengthy terminology; and
- ensure that your subscribers and users understand the information you provide.

You **must not** include ambiguous or unclear references to ‘partners’ or ‘third parties’ in the information you provide.

You **must** consider how the design of your online service impacts on the visibility of the link to your information. For example, a link at the bottom of a concise webpage that has no content ‘below the fold’ is 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.

Our UK GDPR guidance on ‘the right to be informed’ outlines methods you can use to provide privacy information.

Equally, the type of device you use to access your service impacts how you inform users about storage and access technologies. The limited, and sometimes non-existent, physical interfaces on some connected devices can make it challenging to provide the right information. You **could** consider alternative methods of informing users, such as:

- including clear, simple-to-follow informational materials along with the device;
- ensuring the setup process for the device includes the necessary information and controls;
- surfacing the information during its installation process, if the device uses a companion mobile app; or
- providing privacy dashboards in any associated online account.

Further reading — ICO guidance

- [The right to be informed](#)
- [Data protection by design and by default](#)
- [What methods can we use to provide privacy information?](#)
- [Designing products that protect privacy](#)

How do we tell people about storage and access technologies set on websites that we link to?

For example, if you have a presence on a social media network, you are likely to include a link to it somewhere on your service. When someone clicks this link, they will be taken to your page on the network.

The operator of the social media network is itself providing an online service that uses storage and access technologies. It may use these for its own purposes, or for purposes that both you and it jointly decide.

Although you may not directly control the storage and access technologies set by the platform, you do decide whether or not to:

- have a presence on the network in the first place;
- include links to the network in your service, the specific tracking tools the network provides, or both if appropriate; and
- use the network's targeting tools and techniques to reach your users when they visit the platform.

Any use of the tools and techniques of these networks for targeting purposes involves personal data processing. This means that if you decide to use them, then both you and the platform are jointly responsible for determining the purpose and means of this processing of personal data.

Even though these cannot be covered by your service's own consent mechanism, you **should** include in your privacy information:

- references to any social media presence that you may have; and
- state that the platform may use storage and access technologies once they visit there.

You **should** consider that not everyone who accesses your social media presence via your website will be logged-in users of that social media platform. 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.

You **should** provide information about the processing of any personal data within your privacy notice, as well as somewhere on your page on the online platform, even if this is simply a link back to that privacy notice.

Example

A website includes a social media plugin. When a visitor to the website uses the plugin, data is collected and transmitted to the social media provider.

The website operator and social media site are joint controllers for the collection and disclosure by transmission of the visitor's data to the social media provider.

The website operator **must**:

- provide the visitor with the identity of the social media provider
- explain the purpose of the processing; and
- obtain consent.

If you have links on your site to other external services that do not relate to your online service (eg useful references or resources related to the content of your website), you **could**:

- provide links to their privacy information; or
- make it clear to your users that you are not responsible for the use of storage and access technologies on that site.

Can we pre-enable any non-exempt storage and access technologies?

No. You **must not** pre-enable non-exempt storage and access technologies. This is the case even when:

- you think that subscribers and users may be unlikely to agree to them otherwise; or
- you don't think that the technology is that privacy intrusive.

Unless the technology meets one of the exceptions, you **must** seek consent before you use storage and access technologies.

Our expectations for good practice are laid out in the '[Our expectations for consent mechanisms](#)' section.

Example

A website uses localStorage for online advertising purposes on its landing page. It has a consent mechanism that includes the wording:

"By continuing to use our website, you consent to our use of technologies that store or access information on your device".

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

This is because the website has decided to set non-exempt storage and access technologies, and is then seeking the user's agreement afterwards. It is only providing the user with an option to 'continue' rather than a genuine free choice about whether they want to accept or reject.

How long can we store or access information for?

PECR does not specify how long you can use any storage and access technologies for. For example, whether the appropriate duration of a cookie is the length of the session or a different period, like 30 days.

You **should** consider the appropriate duration depending on the circumstances of your online service and the purpose you want to use the technology for.

If the technology involves processing of personal data, you **must** also consider the data protection principles, including purpose limitation and storage limitation.

To help you to determine what is appropriate, you **must** ensure that the duration is:

- proportionate in relation to your intended outcome; and
- limited to what is necessary to achieve your purpose.

In some instances, you may decide a longer duration is appropriate, such as a persistent cookie which stores user preferences for a period of time (eg 90 days, if that is appropriate in the context of your service and its users).

Some storage and access technologies, like cookies, may have a default duration. An expiry limit for persistent cookies may be set by the browser, and in some cases users can remove persistent cookies manually.

Alternatively, if you are storing objects in localStorage, there may be no expiry date.

Whatever technology you are using, you **should** consider:

- what the default is;
- whether this is appropriate; and
- if it is something you can change if necessary. For example, by automatically removing objects in localStorage where appropriate.

In all cases, the key is ensuring a proportionate approach to the purpose. For example, while it may be technically possible to set the duration of a cookie to ‘31/12/9999’, this could not be regarded as proportionate in any circumstances.

Example

An online service sets persistent cookies on its website.

The service recognises that the user’s browser may limit the maximum age of a cookie to 400 days. It decides to use the default expiry date for all of its cookies and relies on the user’s browser to adjust the maximum expiry time.

This is not a proportionate approach, because:

- the service cannot assume that the user’s browser will change the default; and
- a 400 day expiry date may not be appropriate for the purpose of the cookies on its service.

Further reading

- [Principle \(b\): Purpose limitation](#)

- [Draft update to RFC 6265](#) (section 5.5) the W3C document that defines the HTTP cookie (external link).

What is an audit and how can we do one?

You **should** undertake regular reviews of your online service, as well as any storage and access technologies it includes.

The frequency of your reviews depends on:

- the specific storage and access technologies you use;
- the purposes you use them for; and
- how often you change or update them.

For example, if you make regular changes, you should carry out reviews more frequently.

You may decide a comprehensive ‘audit’ of your online service is appropriate. For example if the functionality of your website has evolved over time and multiple staff or teams have editing access to the site.

You **could** take a user’s perspective by visiting your website on a device separate from your network and checking what storage and access technologies are present. You **could** invite a third party to do this on your behalf.

You **should** include the following steps in an audit, depending on the nature of your service and how you provide it:

- identify the storage and access technologies your service currently includes (eg by using a combination of browser-based tools or server-side code reviews);
- confirm the purpose(s) of each of the storage or access technologies you are using (and any new ones you intend to use);
- identify any you no longer need and remove them;
- in any mobile app, identify the installed SDKs and their respective data flows;
- determine whether any of the purposes you use storage and access technologies for meet an exception (and if so, which one) and any that do not, and take appropriate action;
- confirm whether your storage and access technologies are linked to other information held about your users, such as usernames, and whether using them involves (or will involve) processing personal data;
- identify the data that each technology involves, holds or processes;
- determine the lifespan of any persistent cookies, and justify their duration in relation to the purpose(s) you use them for;
- identify whether any third parties are setting storage or access technologies on your site and if so, who and for what purpose;
- review any automatic categorisation of storage and access technologies and whether this is correct;
- review your consent mechanism and privacy settings to ensure that users can reject the use of any non-exempt storage and access technologies as easily as they can accept them;

- review your consent mechanism to ensure that it has the technical capability to allow users to withdraw their consent with the same ease that they gave it;
- review your privacy information to ensure that you provide clear and comprehensive information about each technology you want to use;
- confirm what information you are sharing with third parties and how you explain this to your users; and
- document your findings and follow-up actions, and decide when you will conduct your next audit.

How do we manage consent in practice?

At a glance

- You **must** obtain consent from the subscriber or user for your use of storage and access technologies. If this involves the processing personal data and you are relying on consent, you **must** have the consent of the person whose data you are processing.
- How you request consent for your use of storage and access technologies depends on what the technologies do, and to some extent, the relationship you have with your users.
- You **must** also ensure that you tell your users about any third parties, and that they can access specific information about each one.
- You **should** consider any implementation of banners, pop-ups, message boxes, header bars or similar techniques carefully, particularly in respect of the implications for the user experience.
- You **should** make sure that electronic consent requests are not unnecessarily disruptive.
- You **must** make your consent requests specific to the purpose. This will generally require providing your subscribers and users with granular options about each purpose you want to use storage and access technologies for.
- Neither PECR nor the UK GDPR set a specific time limit on consent. How long your consent lasts will depends on multiple factors.
- If you introduce new storage and access technologies for a different purpose to what you originally stated when consent was granted, you **must** obtain fresh consent for the new technology or purpose.
- If you use a consent management platform (CMP) provider, you **must** consider the roles and responsibilities you both have under the UK GDPR.
- The exceptions in regulation 6 are purpose-specific. This means it can be challenging to use ‘multi-purpose’ storage and access technologies.
- You **must** ensure that any consent mechanism has the technical capability to allow users to withdraw their consent with the same ease that they gave it.

In detail

- [When do we need to get consent?](#)
- [Who do we need consent from?](#)
- [How do we request consent?](#)
- [Can we use pop-ups and similar techniques?](#)
- [Our expectations for consent mechanisms](#)
- [Can we rely on settings-based consent?](#)
- [Can we rely on feature-led consent?](#)

- Can we rely on browser settings and other control mechanisms for consent?
- Can we use ‘terms and conditions’ to gain consent?
- Can we bundle consent requests?
- How often do we need to request consent?
- What if our use of storage and access technologies changes?
- Can we use the same storage and access technology for multiple purposes?
- How do we keep records of user preferences?
- What if a user withdraws their consent?

When do we need to get consent?

If none of the exceptions apply to your use of storage and access technologies, then you **must** obtain prior consent.

Who do we need consent from?

PECR states that you **must** obtain consent from the subscriber or user.

In practice, it can be difficult for you to tell which one provides consent. However, you **must** ensure one of the parties has provided valid consent.

PECR does not specify whether the user’s or subscriber’s wishes should take precedence if people have different preferences about the use of storage and access technologies.

There are some cases where the subscriber’s preferences may take priority.

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.

In a domestic context there is usually one subscriber (the person in the household named on the bill) and potentially several other users.

If a user complains that your website is using storage and access technologies without their consent, you may be able to show that you obtained consent previously from the subscriber to demonstrate compliance with PECR.

But, if your use of storage and access technologies involves processing personal data and you are relying on consent, you **must** have the consent of the person whose data you are processing.

You **should** ensure information about storage and access technologies, and mechanisms for making choices, are as easily accessible as possible to all users.

Further reading — ICO guidance

- [How should we obtain, record and manage consent?](#)
- [What methods can we use to provide privacy information?](#)

How do we request consent?

How you request consent for your use of storage and access technologies depends on:

- what the technologies do; and
- to some extent, the relationship you have with your users.

The key is that you **must** provide clear and comprehensive information so that your users understand what you want their consent for and what choices they have. You **should** consider a variety of techniques to achieve this outcome as appropriate for your service.

For their consent to be valid, you **must** give your users control over all the non-exempt storage and access technologies you use. Any use of a consent mechanism **must** function as intended to ensure that choices made through the mechanism are respected.

You **must** also ensure that you tell your users about any third parties and that they can access specific information about each one. It is your choice to decide the most appropriate way to do this in the context of your service. For example, whether it is appropriate to use layers or panels.

For consent to be valid, you **must** provide the identity of any third parties you share data with. Without this information, subscribers and users cannot determine the consequences of the consent they may give.

If you use a layered approach, you **must** either:

- provide the identities of third parties on the first layer; or
- be able to demonstrate that the user has access to these identities. For example, on a second layer that you clearly and prominently indicate on the first layer.

Any third party who relies on the consent you obtain from your users **must** be able to demonstrate that your users understand you intend to share the data with them, and for what purpose.

In general, any consent you obtain in this context is more likely to be valid if you make an active choice to partner with a particular third party for a specific purpose. It may be challenging for you to meet the requirements of valid consent if you use a large number of third parties on your service.

Can we use pop-ups and similar techniques?

Banners, pop-ups, message boxes, header bars or similar techniques might seem to be the easiest option for you to achieve compliance with PECR — whether that is requesting consent or providing clear and comprehensive information.

However, you **should** 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. This means any consent from people using a mobile may not be valid as the information may be difficult to access.

Similarly, long lists of checkboxes might seem like a way to make your consent mechanism appropriately granular, but this approach carries different risks. This is because your users may simply not interact with the mechanism or understand the information you're providing.

You **should** make sure that electronic consent requests are not unnecessarily disruptive. You **should** consider how you provide clear and comprehensive information without confusing users or disrupting their experience. However, avoiding disruption does not override the need to ensure that consent requests are valid, so some level of disruption may be necessary.

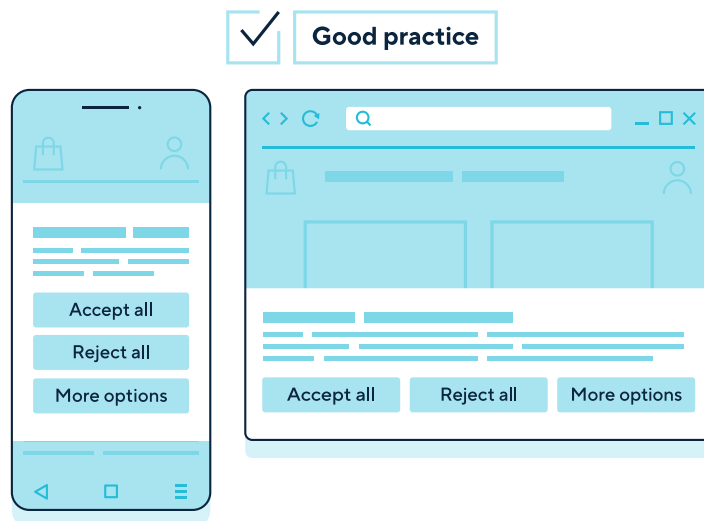
Many online services routinely use pop-ups to make users aware of changes to the website or to ask for their feedback. You **could** use this as a way to highlight the storage and technologies you use.

There are challenges with using these techniques. If users do not click on any of the options available and go straight through to another part of your website, you **must not** use the storage and access technologies that require consent. This is because you **must** ensure the consent involves a positive action. Silence or inactivity doesn't qualify. So, you cannot assume that people who don't engage with your consent mechanism have agreed to the storage and access technologies you want to use.

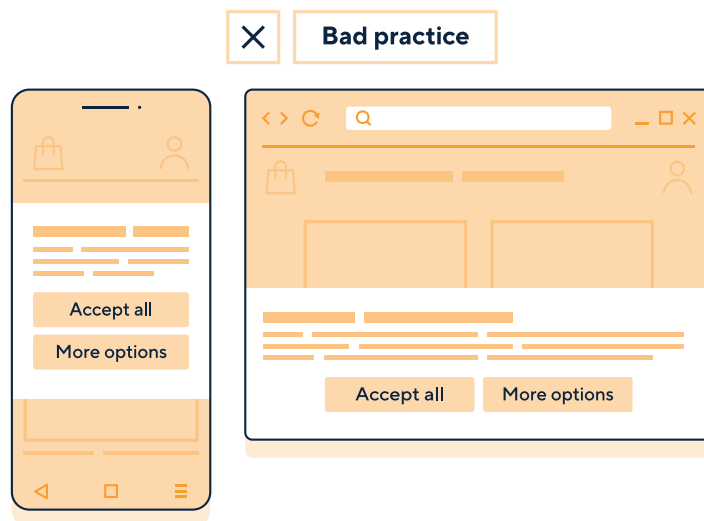
Our expectations for consent mechanisms

This section includes a checklist of key considerations for your consent mechanisms and examples of good and bad practice. Good practice mechanisms are blue and bad practice mechanisms are orange.

Our consent mechanism makes it as easy to refuse consent as it is to accept.



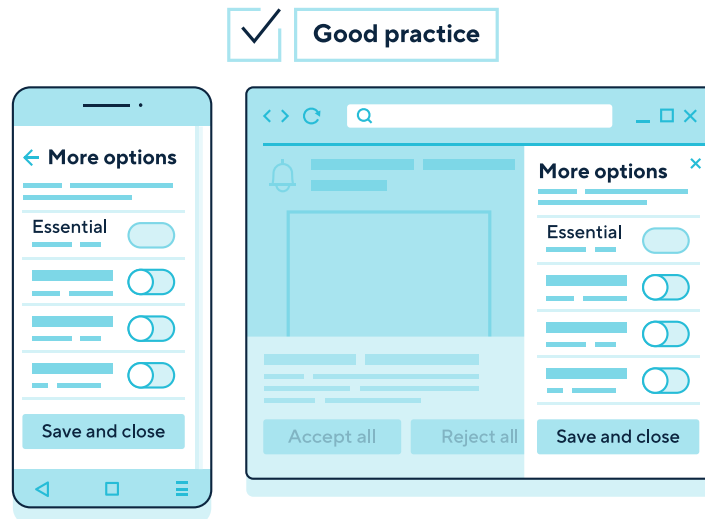
Description: Consent mechanisms on a mobile phone (left) and desktop (right) with equally prominent options to “accept all” or “reject all” non-exempt storage and access technologies, or to customise choices via a “more options” button.



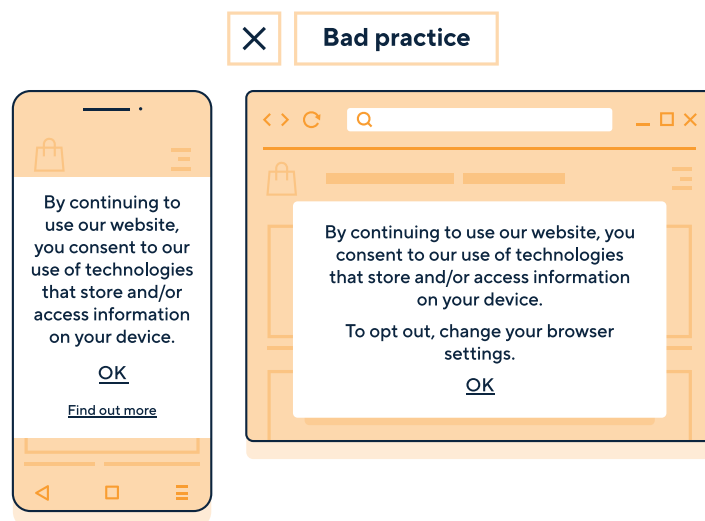
Description: Consent mechanisms on a mobile phone (left) and desktop (right) with options to “accept all” or to customise choices via a “more options” button. There is no option to “reject all” non-exempt storage and access technologies.

□ Our consent mechanism requires a positive action to indicate opt-in from the user, before non-exempt storage and access technologies are set.

□ Our consent mechanism functions as intended. Storage and access technologies are only set when valid consent is gathered, or when they meet an exception.



Description: Example “more options” tabs of consent mechanisms on a mobile phone (left) and desktop (right) with toggles for all non-exempt storage and access technologies turned off by default. A “save and close” button is available to close the mechanism.

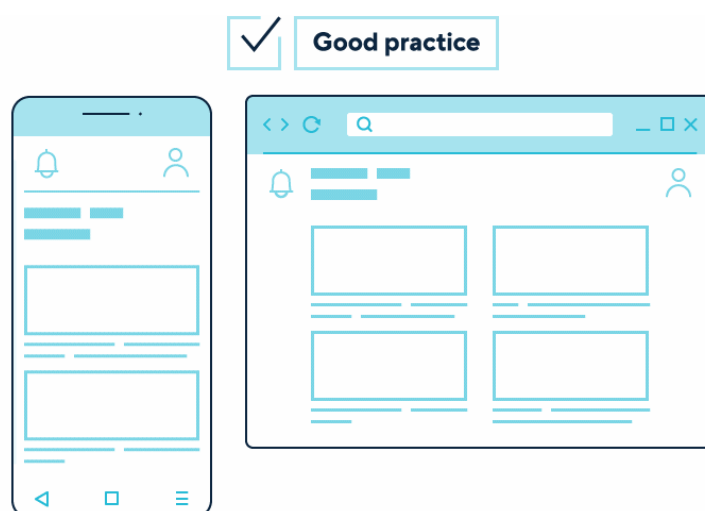


Description: The image on the left shows a pop-up consent mechanism on a mobile phone displaying the text: “by continuing to use our website, you consent to our use of technologies that store and/or access information on your device.” There are two buttons beneath it: “ok” and “find out more.” This is an example of pre-enabling storage and access technologies without consent.

The image on the right shows a pop-up consent mechanism on a desktop displaying the text: “By continuing to use our website, you consent to our use of technologies that store and/or access information on your device. To opt out, change your browser settings.” There is one button beneath it which says “ok”. This is an example of pre-enabling storage and access technologies without consent, and relying on a user to adjust their browser settings to opt out.

❑ Our consent mechanism includes granular options for different purposes.

For consent to be valid, you **must** give your users control over all the non-exempt storage and access technologies you use.



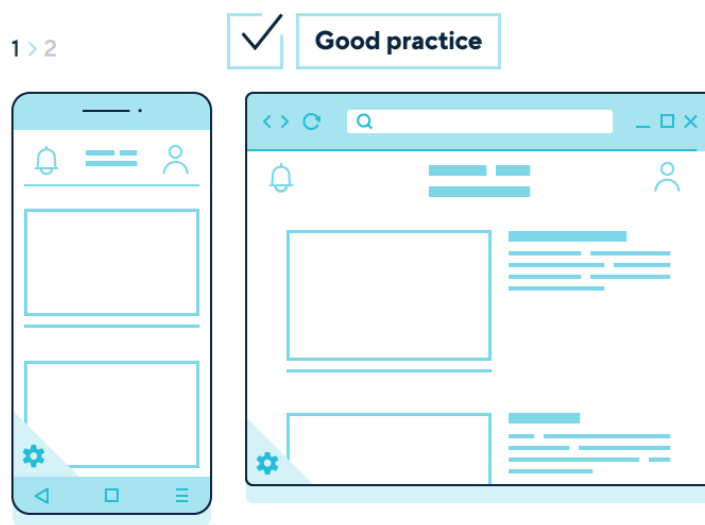
Description: Step 1 shows a pop-up consent mechanism with three equally prominent options for users to “accept non-exempt”, “reject non-exempt” or “customise” the use of storage and access technologies on a mobile phone (left) and desktop (right).

Step 2 shows a user selecting the “customise” option and a second layer of the mechanism appearing. This provides specific descriptions for categories appropriate to the service. In this example, there are four purposes: “essential”, “analytics”, “social media tracking” and “advertising.”

There is no toggle for the “essential” category, but there are toggles for the other three categories. The “analytics” category is on by default. The other two categories are off by default. A button displaying “save and close” stores the user’s preferences.

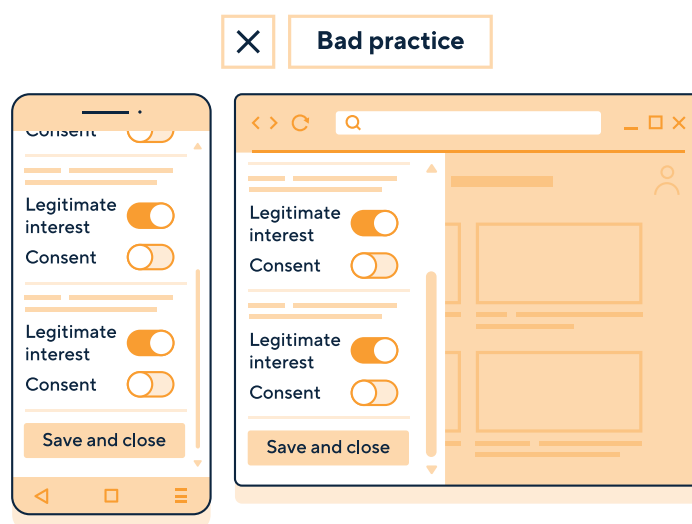
❑ Our consent mechanism informs users about the identities of all third parties their information will be shared with if they grant consent. Users are able to control any information shared with individual third parties.

□ Our consent mechanism informs users about how they can revisit their preferences.



Description: A graphic displayed on a mobile phone (left) and desktop (right). Step 1 displays a webpage with a “settings” icon in the bottom left corner. Step 2 shows a consent mechanism appearing when a user clicks on the “settings” icon. The consent mechanism explains that the “settings” icon allows people to change their preferences at any time. The mechanism can be closed by selecting “save and close.”

□ Our consent mechanism does not incorrectly use legitimate interests as a lawful basis.



Description: Bad practice examples of consent mechanisms on a mobile phone (left) and desktop (right). The mechanisms have purposes listed alongside separate “legitimate interests” and “consent” toggles. The “legitimate interests” toggles are switched on by default and the consent option toggles are switched off by default. A “save and close” button is available.

Can we rely on settings-based consent?

Some storage and access technologies are deployed when a user makes a choice over a site's settings. 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 may involve storage and access technologies, such as 'preference cookies' or 'user interface' cookies.

In practice, it is likely that the use of these technologies falls within the appearance exception and does not require consent.

However, if are using the storage and access technologies for any other purposes beyond the scope of the exception, or if they persist beyond the user's current session, you **must** obtain consent.

In this scenario, you **could** seek consent as part of the process, whereby a user confirms what they want to do or how they want the website to work. For example, by explaining that by allowing their choice to be remembered they are giving their consent in a way that is integrated with the choice the user is already making.

Can we rely on feature-led consent?

In some cases, a user may interact with a feature on your website, such as by choosing to watch an embedded feature or engaging with a chatbot function. At that point, if the user is well informed, it can be considered strictly necessary to provide the service requested by the user.

If this doesn't apply in your circumstances, you **could** obtain consent about particular features of your service at the point where the user engages with them. For example, if an embedded video uses storage and access technologies beyond those that are necessary to provide the content requested by the user.

Regardless of whether you requested consent, you **must** provide clear and comprehensive information because you may process personal data and the UK GDPR will still apply. This includes being clear about when the feature is provided by a third party.

Can we rely on browser settings and other control mechanisms for consent?

PECR states that the controls on an internet browser can be a way in which the subscriber or user may signify their consent.

In a traditional web environment, browsers or similar applications may:

- be set up by their users either to allow or not allow particular storage and access technologies; or
- include certain defaults that prevent their use (eg tracking protection features).

However, you **must not** assume that each visitor to your online service has either configured their browser in this way, or that they use a browser with these protection features.

For consent to be clearly signified in this way, you **must** be certain that the subscriber or user has been prompted to consider their current browser settings. This requires evidence of either a positive action that they are happy with the default, or otherwise decided to change the settings.

In the same way that a website may eventually be able to use browser settings as an indication of valid consent, preference settings within a device's operating system may mature into a consent mechanism for app and web app developers.

But even when browser controls are improved, it is likely not all users will have the most up-to-date browser with the enhanced privacy functionality needed for these settings to constitute an indication of consent.

This means that for now, you **must not** rely solely on browser settings to indicate consent.

Can we use 'terms and conditions' to gain consent?

No. You **must** ensure that consent is separate from terms and conditions.

You **must** obtain consent by:

- giving the user specific separate information about what you want them to agree to; and
- providing them with a way to take a positive action to opt-in.

You **must not** attempt to obtain consent via terms and conditions.

Can we bundle consent requests?

You **must** keep consent requests specific to the purpose.

Generally, this means you **must** provide your subscribers and users with granular options related to each purpose you want to use storage and access technologies for.

Example

A firm offers multiple distinct services to users. As part of its account sign-up process, it asks users to provide a single consent to:

- the processing of their personal data for use in personalising the services they receive (such as personalised recommendations and personalised advertising); and
- set cookies for various purposes, including some not directly related to the personalisation of the account.

The user can therefore consent to all the services offered by that company being personalised and cookies being set or refuse consent for all of them.

The user can change the individual consents at a later date in their account settings. However, by presenting the bundled option initially, the company increases the likelihood of users consenting to all processing activities and reduces the chances that they will withdraw that consent at a later time.

This means the consent to set cookies is unlikely to be valid, as it is not specific or informed.

ICO and CMA joint position paper on harmful design in digital markets

<https://www.drcf.org.uk/publications/papers/ico-cma-joint-paper-on-harmful-design-in-digital-markets/>

How often do we need to request consent?

Neither PECR nor the UK GDPR set a specific time limit on consent. So, how long consent lasts for your use of storage and access technologies depends on multiple factors. These include:

- the scope of the original consent;
- the expectations of your subscribers and users;
- whether your use of particular storage and access technologies has changed since they last consented;
- how frequently people visit your service; and
- how disruptive consent requests may be for them.

Considering these will help you to decide the appropriate duration of any consent (or rejection) and therefore the point at which you ask your subscribers and users for their consent again.

PECR isn't intended to inconvenience or unduly disrupt the experience of your users. You **should not** repeatedly ask or prompt people to specify their preferences as a matter of course. This is particularly the case when someone has refused consent. It is unfair to repeatedly request their consent just because you want them to respond differently.

If a user has declined consent, you **should** only choose to seek their consent after a reasonable amount of time has passed. As a general guideline, we recommend that six months is a suitable timeframe to request fresh consent for the use of storage and access technologies.

There may be circumstances where you need to refresh consent more frequently. For example, you **must** request fresh consent if your purposes or activities change or evolve from what you specified in the original request for consent.

What if our use of storage and access technologies changes?

Your use of storage and access technologies is likely to change over time. For example, you may decide to:

- add or remove particular technologies to your website;
- use existing ones for a new purpose; or
- incorporate new third parties and share information with them.

You **must** consider how these changes impact on:

- the information you provide to your users;
- any consent you have previously gained; and
- your reliance on any of the exceptions, if applicable.

For example, if you introduce new tags or cookies for a different purpose to what you originally stated when consent was granted, you **must** obtain fresh consent for the new purpose.

If you embed services or features from other organisations (eg streaming video), you **should** ensure that you:

- know whether this involves storage and access;
- tell your users about it; and
- are able to configure this feature in the most privacy-preserving way.

Example

A website operator decides to use a consent mechanism that enables the user to:

- consent or refuse non-exempt storage and access technologies; and
- see the names of third parties the website operator shares information with, and for what purposes.

The mechanism stores the user’s choice in a preference cookie for six months. If the user doesn’t visit the site again in that timeframe, the cookie expires.

The website operator adds a new social media plugin to the website. This results in information being collected and disclosed to the social media network.

The website operator recognises that the consent previously obtained does not cover collecting and sharing information with the social media network. It **must** make sure that consent is specific and informed. It also recognises that this purpose will not be within their user’s expectations.

For this reason, it requests fresh consent from its users.

Further reading — ICO guidance

- [Consent](#)
- [Principle \(b\): Purpose limitation](#)

Can we use the same storage and access technology for multiple purposes?

Storage and access technologies may be capable of processing the same information for more than one purpose, depending on their functionalities and how you configure them. But the exceptions in regulation 6 are purpose-specific. This means it can be challenging to use ‘multi-purpose’ storage and access technologies.

If all the purposes meet the requirements of the same exception then you aren’t required to get consent. For example, a particular technology might store and access information for the purposes of ensuring your service’s security as well for the purposes of preventing repeat login prompts on each new page that a user visits. Both of these processing activities are for purposes that are strictly necessary to provide the service.

It is more difficult for you to do something like rely on the strictly necessary exception for one purpose while also relying on the statistical purposes or appearance exceptions for another purpose. This is because these two exceptions only apply where your storage or access is for ‘the sole purpose’ of:

- collecting statistical information to improve the service or website (the statistical purposes exception); or
- enabling the way the service appears or functions when someone accesses it on their device (the appearance exception).

The wording ‘sole purpose’ means that the exceptions only apply where the storage or access is carried out for **that** purpose, as opposed to **any other** purpose at the same time.

Also, if one purpose meets the requirements of an exception but another does not, you **must** get consent for the storage or access. For example, you can’t store or access information for the statistical purposes exception while also using that information for other purposes like online advertising.

Don’t forget that for consent to be valid, you **must** give users control over the non-exempt purposes. Your consent mechanism **must** include granular options for different purposes and you **must** ensure that it functions as you intend it to.

You might prefer to use the same storage and access technology for multiple purposes. But in practice, it may be easier to meet your PECR obligations if you use a separate storage and access technology for each purpose.

How do we keep records of user preferences?

You **must** be able to demonstrate that someone has provided consent. The exact method of doing this is for you to decide as the service provider.

In many cases, service providers use a consent management platform (CMP). The CMP presents information about the storage and access technologies to the user and provides controls for them to make their choice. It can then store records of their consent in digital form.

You **could** build the CMP yourself. Or, you **could** partner with a specialist to provide it on your behalf.

However you obtain consent, you **must** ensure that you appropriately protect any records. A CMP can enable you to accurately record what your users consent to and store this for an appropriate duration.

Many off-the-shelf consent mechanisms also involve preference cookies that are stored in the devices of your subscribers and users. These may have a default expiration period (eg 90 days). As with any other storage and access technologies you use, you **should** take the time to determine whether this default interval is appropriate. It may seem simpler to use the default option, but you **must**:

- assess whether it is right for your circumstances;
- take any required actions to change it if necessary; and
- document your decision.

If you do use a CMP provider, you **must** also consider the roles and responsibilities you both have under the UK GDPR. For example, by determining whether the provider acts on your behalf as a processor, and ensuring that you have an appropriate controller and processor arrangement in place.

What if a user withdraws their consent?

The law says that you **must** enable your subscribers and users to withdraw their consent at any time. You **must** therefore ensure that any consent mechanism has the technical capability to allow users to withdraw their consent with the same ease that they gave it. If your mechanism cannot do this, then it does not comply with the UK GDPR's consent requirements.

You **must** also provide information about how people can withdraw consent within your consent mechanism, and ensure that any storage and access technologies that have already been set can be removed.

You **should** make any effects of withdrawing that consent clear.

If someone withdraws their consent to the use of storage and access technologies, you **must**:

- stop using them;
- cease any processing of personal data the technologies undertake; and
- tell any third parties you are working with that the person has withdrawn their consent.

This is because you cannot rely on another lawful basis for processing, as explained in the section: [‘How does PECR consent fit with the lawful basis requirements of the UK GDPR?’](#).

You **must** interpret a withdrawal of consent as a request for erasure and delete any information you hold on the user that you gathered under that consent. Our right to erasure guidance provides more information on how to comply with this request.

Article 19 of the UK GDPR says that you **must** also notify each recipient the personal data has been disclosed to in reliance on that consent, unless this proves impossible or involves disproportionate effort.

If you are an organisation relying on consent gained by someone else and they inform you that a user has withdrawn that consent, then you **must** interpret a withdrawal of consent as a request for erasure. You **must** delete any personal data you hold about that user that you gathered under that consent.

Our detailed consent guidance provides more detail on recording and managing consent.

Example

A user accepted non-exempt storage and access technologies on a travel website when they were looking to go on holiday. They were happy for the travel company to 'remember' their search criteria each time they visited the website, and for this information to be shared with third parties for the purpose of recommending other services to them.

When returning from their holiday, the user no longer wants to be targeted with related adverts, or for their criteria and purchase history to be stored by the website and shared with third parties.

The user clicks a link in their profile to manage their settings and withdraws their consent for the use of non-exempt storage and access technologies.

Through its consent mechanism, the website notifies any third parties it has shared the personal data with about this withdrawal.

Relevant provision in the UK GDPR - see Article 19

<https://www.legislation.gov.uk/eur/2016/679>

Further reading - ICO guidance

- [Consent](#)
- [Right to erasure](#)
- [Right to be informed](#)

How do the rules apply to online advertising?

At a glance

- The use of storage and access technologies for online advertising purposes requires consent. This applies both in the context of the technical processes involved in ad selection and delivery, as well as any associated tracking and profiling.
- Advertising measurement does not require a **separate** consent, as the collection of information for measuring the effectiveness of campaigns is intrinsically linked to the purpose of online advertising.
- In principle, contextual advertising more readily enables you to comply both with the PECR requirements as well as your UK GDPR obligations than other types of targeted advertising.

In detail

- [Do we need consent for online advertising?](#)
- [Does advertising measurement require consent?](#)
- [What types of online advertising can we use?](#)
- [Can we use 'cookie walls' or 'consent or pay' models?](#)

Do we need consent for online advertising?

Yes. The use of storage and access technologies for online advertising purposes requires consent.

This applies both in the context of the technical processes involved in ad selection and delivery, as well as any associated tracking and profiling.

The use of storage and access technologies for the purposes of online advertising is not strictly necessary to provide a service to the user. This is because on a technical level, the service can be provided without any advertising.

Obviously, service providers also seek to generate revenue from online advertising. But this doesn't make it 'technically unfeasible' to provide the service without it.

If you have process personal data for online advertising purposes based on consent, and then supply the data to third parties, you **must** ensure that the user's consent applies across the chain.

When you ask for consent, you **must** clearly explain to your users:

- who you will share the data with;
- for what purpose; and
- how they can exercise control over this processing.

You, and the third parties involved, **must** ensure you have a process for passing on when a user has withdrawn their consent. In practice, if you have collected the consent, you are responsible for telling the third parties when this consent is no longer valid.

You **must** obtain consent for the use of storage and access technologies where these are used for analysing or predicting people's personal preferences, behaviour and attitudes.

Example

A company offering marketing services obtains personal data from a third-party supplier. It combines this information with its own (first-party data) and public databases and processes it to create individual profiles on people.

The data obtained from a third-party supplier was collected with consent from each person. As the company cannot demonstrate that this processing is fair and lawful without consent, it decides that it cannot rely on the legitimate interests lawful basis to use this data for profiling. Instead, the company goes back to the data supplier to check whether it:

- considers the consent to be valid; and
- has a way to find out if a person has withdrawn their consent.

If either of these conditions are not satisfied, it will not use the data.

Data protection law does not stop you from tracking and profiling people for online advertising purposes. However, you **must** ensure that people:

- are made aware of the processing;
- are given meaningful control over their data; and
- can exercise their rights.

Does advertising measurement require consent?

Yes, but this forms part of the consent you obtain for online advertising purposes.

The requirement for consent applies to any storage and access technology used for online advertising purposes. These purposes can include measurement of the effectiveness of ad campaigns.

The measurement does not require a **separate** consent, as the collection of information for measuring the effectiveness of campaigns is intrinsically linked to the purpose of online advertising.

This means that as long as your use of storage and access technologies is based on the user's consent, you don't need additional consent for measurement purposes.

However, if you do group consent requests for purposes that are intrinsically linked, you **must** provide clear and comprehensive information to your users about these purposes and ensure the consent is valid.

You **must** still follow the rules for refreshing consent where required, such as where new third parties are involved, or if you plan to use the storage and access technologies for a new purpose. This is particularly important in the context of online advertising, where a large number of third parties may be involved in a complex supply chain.

If the information is used for other purposes that are not intrinsically linked to the original purpose, you **must** obtain separate consent. For example, this would be the case if third parties are processing information on a user's interaction with the advert for tracking or profiling people.

What types of online advertising can we use?

This is ultimately a decision for you to take.

There are different types of online advertising. The most common ones involve techniques that target the ads in some way so that a user is more likely to interact with them. For example, ads can be targeted based on:

- the content of the page the user is currently viewing. This is usually known as 'contextual advertising'; or
- the user's known or inferred interests, characteristics and behaviours, particularly over time and potentially across different services, locations and devices. This is usually known as 'behavioural advertising'. It includes a range of targeting techniques that involve profiling the user (eg observing their online activities).

This means most online advertising is 'targeted'. The difference is what the ads are targeted on. It may be common to refer to adverts targeted on the basis of someone's personal data as 'personalised advertising', but you **should** be clear about the specific techniques you intend to use and which of these involve profiling.

In principle, contextual advertising more readily enables you to comply with both your PECR and UK GDPR obligations. While it can still involve personal data processing, this is less extensive than with other types of targeted advertising (eg, those that involve profiling, like behavioural advertising). This is because personal data is not used to determine what advert a user sees.

However, any storage and access technologies used for the purposes of online advertising require consent.

Further reading — ICO guidance

- [Consent](#)
- [A guide to lawful basis](#)

Further reading

- [ICO online tracking work](#)
- [Information Commissioner’s Opinion 2021: Data protection and privacy expectations for online advertising proposals](#)

Can we use ‘cookie walls’ or ‘consent or pay’ models?

A cookie wall, sometimes called a ‘tracking wall’, requires users to ‘agree’ or ‘accept’ the setting of storage and access technologies before they can access an online service’s content.

There are different types of these models. Whether they result in valid consent depends on what model the online service uses and the specific choices it makes about the implementation.

One example is a model that requires the user to ‘agree’ to the tracking, otherwise they cannot access the service at all. This is known as the ‘take it or leave it’ approach.

In most cases, the ‘take it or leave it’ approach does not comply with the requirement for consent to be freely given.

This is because you **must** provide a genuine free choice. You **must not** bundle consent up as a condition of the service unless it is necessary for that service.

A new model is emerging that gives people a choice between:

- accessing online services without payment if they consent to their personal data being used for personalised advertising; or
- having to pay to access that service if they refuse this consent.

This type of access mechanism is typically known as ‘consent or pay’ or ‘pay or okay’.

The issues that this touches on are complex. We have produced specific guidance on ‘consent or pay’.

Further reading

[Consent or pay](#)

What happens if we don't comply?

What happens if we don't comply

Due to the [Data \(Use and Access\) Act](#) coming into law on 19 June 2025, the PECR enforcement regime is changing. We will update this section once the new regime is in force.

Our aim is to ensure organisations comply with the law. In cases where organisations refuse or fail to comply voluntarily, we have a range of options available for taking formal action where this is necessary.

The enforcement regime for PECR is changing to align with the regime for the UK GDPR as laid out in the DPA 2018.

Once these changes are in force, we will produce new guidance on the approach to PECR enforcement. This will replace the Regulatory Action Policy which currently applies to PECR.

In the meantime, the published Regulatory Action Policy still applies to PECR. It makes clear that any formal action we take must be a proportionate response to the issue it seeks to address and that we will reserve monetary penalties for the most serious infringements of PECR.

Further reading — ICO guidance

[Regulatory Action Policy](#)

Glossary

Glossary

- **Application Programming Interface (API):** A computing interface that defines interactions between multiple software intermediaries.
- **Client:** A system or program that requests the activity of one or more other systems or programmes, called servers, to accomplish specific tasks. In a client-server environment, the web user's interface, such as a web browser, is usually the client.
- **Device fingerprinting:** Collecting pieces of information about a device's software or hardware. These can be combined to uniquely identify a particular device.
- **First party:** The online service the subscriber or user is visiting. For example, in a web browser context, if someone visits the website <https://example.com>, Example.com is the first party.
- **HTTP Header:** Additional information passed between a client and a server in an HTTP request or response. For example, in a request header, information is provided about the request context, such as what browser is being used, so that the server may provide a correct response.
- **JavaScript:** A dynamic programming language used for web development.
- **Persistent storage:** When information is stored between browser sessions and can therefore have a longer duration.
- **Server-side solutions:** Where data received from the client-side is further processed and distributed to various tag partners on a remote server.
- **Session:** A 'session' refers to a certain timeframe for communication between two devices, two systems or two parts of a system. For example, session cookies generally expire when someone closes their browser or shortly afterwards.
- **Session storage:** When information is stored for the duration of a 'session'. For example, session cookies generally expire when someone closes their browser or shortly afterwards.
- **Software Development Kit (SDK):** A set of tools used for developing applications provided by hardware and software providers. They usually include application programming interfaces (APIs), sample code and documentation.
- **Subscriber:** A person who is party to a contract with a provider or public electronic communications services for the supply of such services.
- **Third party:** An organisation that is distinct from the online service the subscriber or user is currently visiting. For example, in a web browser context, if someone is visiting the website <https://example.com>, for analytics services provided by <https://analytics.com> about visitors to <https://example.com>, <https://analytics.com> is considered a third party.
- **Tracking pixel:** Small pieces of code, usually an image file, embedded into a piece of content like a website or an email. Their purpose is to create a communication between the

user's client (eg a web browser) and a server. May also be called: web beacon, web bug, tracking bug, tag, web tag, page tag, pixel tag, 1×1 GIF, spy pixel or clear GIF.

- **User:** Any person using a public electronic communications service.
- **Web server:** The central location that hosts web pages or a website and enables a remote 'client' to access the material held.

Further reading — ICO guidance

[Key concepts and definitions](#)