ABOUT COOKIES:

A cookie is a very small text file placed on an internet user's hard drive. It is generated by a web page server, which is basically the computer that operates a website. The information the cookie contains is set by the server and it can be used by that server whenever the user visits the site. A cookie can be thought of as an internet user's identification card, which tell a website when the user has returned.

How to manage and delete cookies

How to manage and delete cookies in the most common browsers.

Web browsers give users control over what cookies are stored, but each works slightly differently. Follow these instructions to find out how to delete and manage cookies in your browser.

GOOGLE CHROME:

Clear, enable, and manage cookies in Chrome - Computer - Google Chrome Help

SAFARI iPhone:

Clear the history and cookies from Safari on your iPhone, iPad or iPod touch – Apple Support (UK)

MOZILLA FIREFOX:

Protect your privacy | Firefox Help (mozilla.org)

MICROSOFT EDGE:

Microsoft Edge, browsing data, and privacy

INTERNET EXPLORER:

Delete and manage cookies (microsoft.com)

Cookie FAQs

What is a cookie?

The cookie itself is a very small text file placed on an internet user's hard drive. It is generated by a web page server, which is basically the computer that operates a website. The information the cookie contains is set by the server and it can be used by that server whenever the user visits the site. A cookie can be thought of as an internet user's identification card, which tell a website when the user has returned.

What does a cookie look like?

Below is the content of a typical cookie. This one is from the Hotmail service and has the filename jss@hotmail.msn.txt (.txt is the standard filename extension for text files):

HMP1 1 hotmail.msn.com/ 0 1715191808 32107852 1236821008 29449527 *

The codes will only make sense to Microsoft's MSN Hotmail servers.

History of cookies

Cookies for the internet were originally developed in 1995 by browser company Netscape. The word 'cookie' comes from 'magic cookie,' a term in programming languages for a piece of information shared between co-operating pieces of software. The choice of the word cookie appears to come from the American tradition of giving and sharing edible cookies.

What is the purpose of cookies?

Cookies make the interaction between users and websites faster and easier. Without cookies, it would be very difficult for a website to allow a visitor to fill up a shopping basket or to remember the user's preferences or registration details for a future visit.

Websites use cookies mainly because they save time and make the browsing experience more efficient and enjoyable. Websites often use cookies for the purposes of collecting demographic information about their users.

Cookies enable websites to monitor their users' web surfing habits and profile them for marketing purposes, for example to find out which products or services they are interested in and send them targeted advertisements.

Different types of cookies

Session or transient cookies

Cookies that are stored in the computer's memory only during a user's browsing session and are automatically deleted from the user's computer when the browser is closed.

These cookies usually store a session ID that is not personally identifiable to users, allowing the user to move from page to page without having to log in repeatedly. They are widely used by commercial websites for example, to keep track of items that a consumer has added to a shopping basket.

Session cookies are never written on the hard drive and they do not collect any information from the user's computer. Session cookies expire at the end of the user's browser session and can also become no longer accessible after the session has been inactive for a specified length of time, usually 20 minutes.

Permanent, persistent, or stored cookies

Cookies that are stored on the user's computer and are not deleted when the browser is closed. Permanent cookies can retain user preferences for a particular website, allowing those preferences to be used in future browsing sessions.

Permanent cookies can be used to identify individual users, so they may be used by websites to analyse users' surfing behaviour within the website. These cookies can also be used to provide information about numbers of visitors, the average time spent on a particular page and generally the performance of the website. They are usually configured to keep track of users for a prolonged period, in some cases many years into the future.

Flash cookies

Adobe Flash is not as common as it used to be, but websites that use Flash for video clips or animations will store small files on your computer that are known as Local Shared Objects (LSOs) or Flash cookies. They can be used for the same purposes as regular cookies.

Flash cookies can also back up the data that is stored in a regular cookie. When you delete cookies using your browser controls, your Flash cookies are not affected. So, a website that served a cookie to you may recognise you on your next visit if it backed up its now-deleted cookie data to a Flash cookie.

You can control Flash cookies. Adobe's website offers tools to control Flash cookies on your computer.

Are cookies dangerous?

No. Cookies are small pieces of text. They are not computer programs, and they can't be executed as code. Also, they cannot be used to disseminate viruses, and modern versions of both Microsoft Internet Explorer and Netscape browsers allow users to set their own limitations to the number of cookies saved on their hard drives.

Can cookies threaten users' privacy?

Cookies are stored on the computer's hard drive. They cannot access the hard drive - so a cookie can't read other information saved on the hard drive, or get a user's e-mail address etc. They only contain and transfer to the server as much information as the users themselves have disclosed to a certain website.

A server cannot set a cookie for a domain that it is not a member of. Despite this, users quite often find in their computer files cookies from websites that they have never visited. These cookies are usually set by companies that sell internet advertising on behalf of other websites. Therefore, it may be possible that users' information is passed to third party websites without the users' knowledge or consent, such as information on surfing habits. This is the most common reason for people rejecting or fearing cookies

EU cookie law

Websites in the EU which use lines of browser-readable text known as cookies can only do so with users' consent, and they must provide information about the use to site users.

The EU's E-Privacy Directive of 2002 required that website visitors be given certain information about cookies.

From 26 May 2011 the law changed meaning that in addition to the provision of certain information visitors must give their consent to the placing of cookies. In the UK this change was implemented by the Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2011 (PECR).

From 25 May 2018 the General Data Protection Regulation (GDPR) came into force. It says that consent for data processing has to be given by users through a "clear affirmative action" and it must be freely given, specific, informed and unambiguous.

Because each EU country has some discretion in how it implements a Directive, the cookie laws in other European countries may differ from those of the UK which are set out in PECR.

PECR

The relevant rules are found in amended regulation 6, which reads as follows:

6. - (1) Subject to paragraph (4), a person shall not store or gain information, or to gain access to information stored, in the terminal equipment of a subscriber or user unless the requirements of paragraph (2) are met.

(2) The requirements are that the subscriber or user of that terminal equipment -

(a) is provided with clear and comprehensive information about the purposes of the storage of, or access to, that information; and

(b) has given his or her consent.

(3) Where an electronic communications network is used by the same person to store or access information in the terminal equipment of a subscriber or user on more than one occasion, it is sufficient for the purposes of this regulation that the requirements of paragraph (2) are met in respect of the initial use.

(3A) For the purposes of paragraph (2), consent may be signified by a subscriber who amends or sets controls on the internet browser which the subscriber uses or by using another application or programme to signify consent.

(4) Paragraph (1) shall not apply to the technical storage of, or access to, information -

(a) for the sole purpose of carrying out the transmission of a communication over an electronic communications network; or

(b) where such storage or access is strictly necessary for the provision of an information society service requested by the subscriber or user.

What does this mean?

PECR means that a website operator must not store information or gain access to information stored in the computer or other web-enabled device of a user unless the user "is provided with clear and comprehensive information about the purposes of the storage of, or access to, that information" and "has given his or her consent". The consent requirement in the UK Regulations replaces the previous position which provided that visitors should be given the option to refuse cookies.

The only cookies that do not need users' consent are those that are necessary to fulfil the user's request. That will cover, for example, the use of cookies to remember the contents of a user's shopping basket as they move between pages on a website. Other cookies, including those used to count visitors to a site and those used to serve advertising, will require consent. So will third party cookies that are used on the website.

The consent requirement has been the subject of much discussion but it is difficult to see how anything other than prior consent will comply with the wording of the UK Regulations.

ICO guidance says: "If you do need consent, then – to be valid – consent must be knowingly and freely given, clear and specific…it must involve some form of very clear positive action – for example, ticking a box, clicking an icon, or sending an email – and the person must fully understand that they are giving you consent."

The GDPR says that consent is "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 phrase "by a statement or by a clear affirmative action" was newly introduced by the GDPR and increases the burden on organisations to ensure that a user has taken a specific, measurable action to give consent, such as ticking a box or clicking to accept a message.

Its cookies guidance says: "You need to be confident that your users fully understand that their actions will result in specific cookies being set, and have taken a clear and deliberate action to give consent. This must be more than simply continuing to use the website. To ensure that consent is freely given, users should be able to disable cookies, and you should make this easy to do."

Although the ICO's guidance suggests a number of methods to obtain consent it stops short of providing definitive guidance on how to achieve compliance, leaving it to businesses and organisations to review their use of cookies and consider how they might be able to obtain the necessary consent.

Both the ICO and the UK government have not ruled out the use of browser settings to achieve compliance in the future, but the ICO advises businesses to obtain consent some other way.

The guidance states: "At present, most browser settings are not sophisticated enough to allow you to assume that the user has given consent to allow your website to set a cookie. Also, not everyone who visits your site will do so using a browser. They may, for example, have used an application on their mobile device. So, for now we are advising organisations which use cookies or other means of storing information on a user's equipment that they have to gain consent some other way".

As a result, a number of companies have developed cookie tools and privacy management software which allow an individual to set their cookies preferences by enabling them, for example, to reject the use of analytical, marketing or advertising cookies. Such tools are also a mechanism through which the website owner can seek to obtain and record the individuals' consent so that they can evidence such consent at a later date. These tools also allow an individual to change their preferences. This is important as an individual has the right to withdraw their consent as easily as they have given it. As such tools and software are relatively new to the market they have not as yet been given any regulatory or supervisory authority approval.

Penalty for non-compliance

The Commissioner's Data Protection Regulatory Action Policy sets out the ICO's approach on sanctions. In deciding whether enforcement action is appropriate the ICO will be concerned with the impact of the breach of the cookie law on the privacy and other rights of website users, not just with if there has been a technical breach of PECR.

PECR currently carries a maximum fine of £500,000 for serious breaches. It is anticipated that this power will only be used in limited circumstances. Before this the fine was £5,000 and companies may have been willing to run the risk but with these increased powers the result of enforcement action is potentially more severe.

A new ePrivacy Regulation is currently being debated within Europe. Under this proposal the fines under PECR are likely to come into line with the fines now available under the UK Data Protection Act 2018, which implements the GDPR. The fines will then be substantially higher.

It is important to remember that consent under PECR applies where a cookie, other than a strictly necessary cookie, is used irrespective of whether personal data is collected by that cookie.

The Data Protection Act can also apply

The UK's Data Protection Act of 2018 derives from the GDPR and demands that where personal information is collected then data subjects, including internet users, should be told of this collection or information about it should be made available to them.

Even where it is possible to anonymise information, the information may still be classed as personal data under the Act if it can be traced back or put together with other information to identify the individual.

Therefore, the requirements of the 2018 Act are that the owner of a website using cookies, the controller, must make its identity clear, the purposes for it having the information and anything else necessary in the circumstances to make the processing fair. This information must also be provided when personal data are collected from third parties.

Collection of personal data must be for explicit purposes; the data must be kept up to date, and consent for it must be freely given and clear.

How to comply with EU cookie law

EU law says that organisations using cookies on their websites, which is almost all organisations, must inform users about cookies and obtain their consent for using them. What does that mean in practice?

The EU's E-Privacy Directive of 2002 required that website visitors be given certain information about cookies. From 26 May 2011 the law changed meaning that in addition to the provision of certain information visitors must give their consent to the placing of cookies.

In the UK the laws that give effect to the EU legislation are the Privacy and Electronic Communications (EC Directive) 2003 as amended by the Regulation of 2011 (PECR).

When EU cookies law changes were implemented in 2011 there was some confusion about how websites should seek and get cookie consent. Most sites used a notice for first-time visitors which sought to obtain consent and assumed consent if someone continued to use the site without expressing a preference.

From 25 May 2018 the General Data Protection Regulation (2018 Act) came into force. It says that consent for data processing has to be given by users through a "clear affirmative action" and it must be freely given, specific, informed and unambiguous. It is harder to satisfy these consent requirements and means that the user should be given a real choice about which cookies, other than strictly necessary cookies, are used when they browse the website.

In addition to fulfilling the consent requirements information should be provided to the user in a privacy policy, a data protection notice, or both. The privacy policy or notice if used properly can meet the information provision requirements of both PECR and the 2018 Act.

Obtaining users' consent to the placing of a cookie is technically more difficult. The ICO guidance suggests a number of different ways to obtain consent. This guidance has yet to be updated by the ICO so the suggestions below are a starting point, as any mechanism used will also need to satisfy the requirements of consent under the 2018 Act:

- pop ups or similar techniques asking for consent can be used. Pop ups are discouraged by Web Content Accessibility Guidelines. They may also spoil the experience of using a website. Users can also block pop ups by default, making this impractical;
- preferences that users choose when visiting a site can also be used as a means of obtaining consent. Consent could be gained as part of the process by which the user confirms what they want to do or how they want the site to work, provided sufficient information about the use of the cookies is provided. This would apply to any feature where a user is told that a site can remember certain settings they have chosen;
- website features, such as videos, that remember how users personalise their interaction can also determine user consent. In this case, where the user is taking some action to tell the webpage what they want to happen - opening a link, clicking a button or agreeing to the functionality being 'switched on' - then their consent to set a cookie can be asked at this point;
- for use of analytic cookies to gather information about how people access and use a site it may be possible to add a footer or header to a webpage containing text. This text is highlighted or turned into a scrolling piece of text when a site wants to set a cookie on a user's device. In turn this could direct the user to read additional information, possibly contained in a privacy policy, and make an appropriate choice;
- where a site allows a third party to set cookies the process of getting consent is more difficult. Initiatives that seek to ensure that users are given more and better information about the use of information, for example the use of the "i" symbol, referred to below, should be used. Anyone whose

site uses or allows third party cookies must ensure that the right information is delivered to users so they can make informed choices.

All of the above mechanisms are used to varying degrees of success across websites. Whichever method you choose, cookies should not drop until the user takes some form of positive action on the website.

To try to satisfy the new consent requirements under the 2018 Act, a number of companies have developed cookie tools and privacy management software which allow an individual to set their cookies preferences by enabling them, for example, to reject the use of analytical, marketing or advertising cookies. Such tools are also a mechanism through which the website owner can seek to obtain and record the individuals' consent so that they can evidence such consent at a later date. These tools also allow an individual to change their preferences. This is important as an individual has the right to withdraw their consent as easily as they have given it. As such tools and software are relatively new to the market they have not as yet been given any regulatory or supervisory authority approval.

As an alternative business may wish to consider using a non-cookie site. A simple brochure-style site with no way to login and no e-commerce functionality may not use cookies, meaning that the new law will not affect the site.

Very few sites do this as it could place them at a competitive disadvantage to competitors and sites outside the EU. A non-cookie site may lose revenues from advertising meaning that it is not cost effective to run such a site, and the site would not be able to measure traffic or learn about its users via tools such as Google Analytics, which is cookie-dependent.

Website owners/businesses should consider what would work for them by looking at their business and how they use their website.