

Cookies - regulatory requirements

This guide sets out the rules that apply to the use of cookies. A cookie is a small file made up of letters and numbers, which is downloaded on to a user's computer, smartphone or mobile internet device when they access your website. Cookies allow a website to recognise a user's device. They are an important element of internet usage as they are used to store site preferences and passwords of users. They are also used for online behavioural advertising, eg targeting advertisements at web users based on their previous web browsing history.

The law regulates the circumstances in which an electronic communication service provider, such as a website operator, can store or gain access to information stored in the computer equipment of an individual user.

What are cookies?

A cookie is a small file made up of letters and numbers, which is downloaded on to a device when the user accesses certain websites. Cookies allow a website to recognise a user's device. Guidance issued by the Information Commissioner's Office (ICO) in the UK describes different types of cookies, each of which is explained below.

Session cookies

Session cookies are one of the less intrusive types of cookie because they expire when the user finishes browsing and they are not stored longer than this. These are often used to remember what a user has put into their internet shopping basket or for security when a user is accessing internet banking.

Persistent cookies

Persistent cookies are stored on a users' device after they have finished using a website. They allow the preferences or actions of the user to be remembered, eg for the next time they browse the website or to target advertising.

First and third party cookies

First party cookies are set by a website visited by the user, ie the website displayed in the uniform resource locator (URL) window.

Third party cookies are set by a website other than the one being visited by the user. If your website displays content from a third party, this third party may be able to track how people use your site and set their own cookies on your users' computers. The ICO advises anyone whose website allows or uses third party cookies to make sure that they are doing everything they can to get the right information to users, and that they are allowing users to make informed choices about what is stored on their device.

The need for consent

You cannot use cookies unless you:

- o tell people the cookies are there
- o explain what the cookies are doing
- o obtain their consent to store a cookie on their device

Before the current regulations were introduced, cookies could be stored so long as the website user or internet subscriber was given the opportunity to refuse, ie in the past the user was given the right to opt out but now they must opt in to the use of cookies. This is explained in more detail below.

Law governing use of cookies

Revisions to ePrivacy Directive

The new regime governing the use of cookies reflects Article 5(3) of the EU Directive on Privacy and Electronic Communications (Council Directive (EC) 2002/58) as amended by Council Directive (EC) 2009/136. This law means that every country in the EU should have its own cookie laws. Some countries missed the deadline to bring in their new laws. Other countries added extra requirements on top of the Directive. The new amendment altered what was previously the user's right to refuse cookies so that website operators now actually have to obtain a user's consent to the storage of cookies/information on their computer equipment.

Amended UK regulations

The revised Directive was implemented in the UK by amendments to existing UK Privacy and Electronic Communications (EC Directive) Regulations 2003 (SI 2003/2426) (the 2003 Regulations). These were amended by the Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2011 (SI 2011/1208). Regulation 6 of SI 2011/1208 means that: