

USE OF COOKIES & THE EU COOKIE LAW

Question: What is a cookie?

Answer: A cookie is a little text file composed of alphanumeric characters, which is created on your computer when your browser accesses a website that uses cookies. The files are used to help your browser navigate the website and fully use all its features like logins, preferences, language settings, themes, among other common features. The cookie is used solely to help your browser process a website; it does not collect any information from your computer or snoop on your files.

Cookie files are typically stored in the cookie file of your browser. Each file normally contains:

- The name of the website server that created the cookie
- The duration of the cookie-how long your browser can use the cookie information to access the website that created the cookie
- A cookie value-this unique information is normally a randomly generated number

The server that created the cookie uses the cookie value to remember you when you come back to the site or navigate from one page to another. Only the server that created the cookie can read and process the cookie. Cookies can expire at the end of a browser session (from when a user opens the browser window to when they exit the browser) or they can be stored for longer.

The Regulations apply to both types of cookies:

Session cookies – allow websites to link the actions of a user during a browser session. They may be used for a variety of purposes such as remembering what a user has put in their shopping basket as they browse around a site. They could also be used for security when a user is accessing internet banking or to facilitate use of webmail. These session cookies expire after a browser session so would not be stored longer term. For this reason session cookies may sometimes be considered less privacy intrusive than persistent cookies.

Persistent cookies – are stored on a user's device in between browser sessions which allows the preferences or actions of the user across a site (or in some cases across different websites) to be remembered. Persistent cookies may be used for a variety of purposes including remembering users' preferences and choices when using a site or to target advertising.

First and third party cookies – Whether a cookie is 'first' or 'third' party refers to the website or domain placing the cookie. First party cookies in basic terms are cookies set by a website visited by the user - the website displayed in the URL window. Third party cookies are cookies that are set by a domain other than the one being visited by the user. If a user visits a website and a separate company sets a cookie through that website this would be a third party cookie.

Question: Does OpenLink Financial LLC use Cookies on its website, www.openlink.com?

Answer: Yes. OpenLink Financial LLC uses first party cookies on the OpenLink Financial LLC Website. We tell you about our cookie use in our Privacy Policy found at <http://www.openlink.com/software/about/privacy-policy.html>


How to remove cookies in Internet Explorer 8

1. Exit Internet Explorer 8, and then exit any instances of Windows Explorer.
2. Do one of the following:
 - In Windows Vista or Windows 7, click the **Start** button, type `inetcpl.cpl` in the Start Search box, and then press ENTER.
 - In Windows XP, click Start, click **Run**, type `inetcpl.cpl` in the Open box, and then press ENTER.
3. On the General tab, click **Settings**, and then click **View Files**.
4. Select the files (cookies) that you want to delete.
5. On the **File** menu, click **Delete**.


How to remove cookies in FireFox3

1. Click on **Tools**, then **Options**
2. Select **Privacy**
3. Do one of the following:
 - a. If your **Firefox will** setting is configured to **Remember History**, click the **remove individual cookies** link.
 - b. If your **Firefox will** setting is configured to **Use custom settings for history**, click the **Show Cookies** button.
4. Select the cookie entry in the list and click on the **Remove Cookie** button

How to remove cookies in Chrome

1. Click the wrench icon  on the browser toolbar.
2. Select **Options (Preferences** on Mac and Linux; **Settings** on Chrome OS).
3. Click the **Under the Hood** tab.
4. Click **Content settings** in the "Privacy/Cookies" section.
5. Click the **All Cookies and site data...** button
6. Select the files (cookies) that you want to delete.
7. Click the **X** to the right of the cookie name.

How to remove cookies in Safari

1. Click the Action menu icon 
2. Select **Preferences**
3. Select the **Security** tab
4. Click the **Show Cookies** button
5. Select the files (cookies) that you want to delete.
6. Click the **Remove** button

Question: What is the EU Cookie Law?

Answer: The Privacy and Communications (EC Directive)(Amendment) Regulations 2011 (UK Regulations) was recently amended on May 26, 2011 and 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 program 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.

Note that the previous rule on using cookies for storing information required a site to:

- tell people how the site used cookies; and
- tell them how they could 'opt out' if they object.

Many websites did this by putting information about cookies in their privacy policies and giving people the possibility of 'opting out'.

The new requirement is essentially that cookies can only be placed on machines where the user or subscriber has given their *prior* consent.

Question: When does the EU Cookie Law go into effect?

Answer: The new regulation went into effect on May 26, 2011. Organizations need to take action to comply by no later than May 26, 2012.

Question: What is consent?

Answer: As per Section 5 of the Information Commissioner's Office's Guidance (located at www.ico.gov.uk) on the rules on use of cookies and similar technologies, consent is defined as any freely given specific informed indication of a user's wishes by which the

data subject signifies their agreement to personal data relating to the user being processed. There must be a form of communication where the user knowingly indicates consent/acceptance. This may involve clicking on an icon, sending an email or subscribing to a service. The crucial consideration is that the user must fully understand that by the action in question, they will be giving their consent.

Implied consent:

The level of consent required for any activity has to take into account the degree of understanding and awareness the person being asked to agree has about what they are consenting to. A reliance on implied consent in any context must be based on a definite shared understanding of what is going to happen in this situation a user has a full understanding of the fact cookies will be set, is clear about what cookies do and signifies their agreement. At present evidence demonstrates that general awareness of the functions and uses of cookies is simply not high enough for websites to look to rely entirely in the first instance on implied consent. As consumer awareness increases over the next few years it may well be easier for organizations to rely on that shared understanding to a greater degree. This shared understanding is more likely to be achieved quickly if websites make a real effort to ensure information about cookies is made clearly available to their users, for example, displaying a prominent link to 'More information about how our website works and cookies' at the top of the page rather than through a privacy policy in the small print.

Consent from the user or subscriber:

The Regulations state that consent for a cookie should be obtained from the subscriber or user. The subscriber means the person who pays the bill for the use of the line. The user is the person using the computer or other device to access a website.

In practice the owner of a website may well not be able to distinguish between consent provided by the subscriber or the user. The key then is that valid consent has been provided by one of the parties.

The Regulations do not specify whose wishes should take precedence if they are different. Other references in the legislation to a subscriber's ability to make decisions in this area, such as around browser settings, might suggest the subscriber's indications may in the first instance take priority. There may well be cases where a subscriber, for example, an employer, provides an employee with a terminal at work along with access to certain services to carry out a particular task, where to effectively complete the task depends on using a cookie type device. In these cases, it would not seem unreasonable for the employer's wishes to take precedence. There are other areas of the legislation, around browser settings where the subscriber clearly has the ability to make a decision on behalf of any users. However, there will be circumstances where a user's wish should take precedence. To continue the above example, an employer's wish to accept such a device should not take precedence where this will involve the unwarranted collection of personal data of that employee.

Question: Does the consent rule apply to every type of cookie?

Answer: According to All About Cookies (located at <http://www.allaboutcookies.org/privacy-concerns/new-european-laws.html>), which acts as a free Cookie resource providing the latest information in response to the Information Commissioners Office press issue, the only exception to EU Cookie Law is if what you are doing is 'strictly necessary' for a service requested by the user. This exception needs to be interpreted quite narrowly because the use of the phrase "strictly necessary" means its application has to be limited to a small range of activities and because your use of the cookie must be related to the service requested by the user. *Indeed, the relevant recital in the Directive on which these Regulations are based refers to services "explicitly requested" by the user. As a result our interpretation of this exception therefore has to bear in mind the narrowing effect of the word "explicitly"*. The exception would not apply, for example, just because you have decided that your website is more attractive if you remember users' preferences or if you decide to use a cookie to collect statistical information about the use of your website.