New Rules on Use of Cookies in the UK and EU

June 12, 2012
Attorney Articles

On 26 May 2012, the 12 month lead-in period for the implementation of the Privacy and Electronic Communications (EC Directive) Regulations 2003 (the "UK Regulations") ended. The UK Regulations were introduced in response to the EU's amendments to the Privacy and Electronic Communications Directive (the "E-Privacy Directive"). The amendments to the E-Privacy Directive changed the EU's approach to cookies, seeking to raise users' awareness of the types of information collected by websites and requiring users to consent to the collection of such information.

What are cookies?

Cookies are small files downloaded onto a user's device when a user accesses a website that permit the storage of information. Cookies may be programmed to collect any type of information that a user inputs online, for example, tracking and analysing users' browsing histories and habits and remembering login details or the items in a shopping cart.

There are several different types of cookies including: (i) session cookies used and retained for only one browsing session on a website; (ii) persistent cookies used and retained in between browsing sessions on a website so that a website may remember certain information next time a user visits; and (iii) flash cookies used to enable a media player to work on the user's device.

Consent

Previously the law operated on an 'opt-out' system providing that a user must have an opportunity to refuse the use of cookies on a website. If a user did not refuse cookies could be used.

The E-Privacy Directive now provides that "a user must be asked to give their prior informed consent to receive cookies, unless the cookie is strictly necessary to receive the service which has been explicitly requested by the user." A website operator must therefore explain and provide a user the chance to consent or "opt-in" to the use of such cookies.

The exception of 'strictly necessary' cookies 'explicitly requested' by a user refers to those cookies which are considered essential for a website to provide its services. An example is a cookie embedded on a user's computer to remember what items are placed in an online shopping basket. The UK Information Commissioner's Office ("ICO") has indicated that it will interpret this exception narrowly.

Timing of consent

Authors

Barry D. Glazer
Ron Moscona

Related Services

Europe

Privacy and Social Media

Related Offices

London

The UK Regulations are silent on the timing of obtaining informed consent and do not specifically refer to “prior” consent. The ICO states in its guidance that it is difficult to see that a good argument could be made that agreement to an action could be obtained after the occurrence of the activity for which the agreement is needed. Although the ICO is sensitive to the fact that certain websites set cookies as soon as a user accesses the website, wherever possible consent should be sought prior to any cookies being set.

Jurisdiction of the E-Privacy Directive

In a prior non-binding opinion relating to behavioral advertising, a committee of national data privacy authorities took the view the requirements of the E-Privacy Directive apply when the website is accessible by users in the EU. While doubts may exist as to the implications of such a broad jurisdictional reach given the practical inability of enforcing the regulations against companies not established in the EU, non-EU companies which either have a physical establishment or office in one of the EU countries or specifically target their websites to users in the EU are likely to fall within the jurisdiction of the law and be required to comply with the new requirements.

How to comply with the UK Regulations

There are a number of steps a website operation can take to comply with the UK Regulations.

Cookie audit: conduct a cookie audit to assess what types of cookies are used and how they are used. An audit may also consider whether any cookies on a website are redundant, and so can be removed, and which cookies are essential to enable a website to work properly, thus falling into the ‘strictly necessary’ exception.

Third party cookies: website operators should not only be aware of their own cookies on their websites but also those served by third parties, such as advertisers. If the user has previously consented to the third party’s cookie, consent is not required for the use of the cookie on another website.

Risk to a user’s privacy: assess how intrusive a website’s use of cookies is. The more intrusive the cookie is, the greater the perceived risk to the user and so the more likely that a website operator will require consent for its use.

Solutions for obtaining consent: The ICO has identified several methods of obtaining consent. While the methods employed by website operators may vary, it is important that such methods notify a user of the use of cookies, provide a user with information about the cookies and the opportunity to explicitly consent to such use, if necessary. A website operator should consider which method is most appropriate for its website taking into account the requirements of the UK Regulations, contents of the ICO’s guidance and the quality of a user’s experience on its website.

- Browser Settings: Browser settings may be programmed to permit the use of certain types or all cookies. This potentially could negate the need for a website to obtain consent through other methods. At present, most browser settings are not sophisticated enough to do this. However the ICO and UK government are working with browser providers to develop and test this technology. Hopefully this will be a viable means of obtaining consent sooner rather than later.
- Pop-ups/ drop-down accordion: Although this is probably the easiest option to

obtain prior consent, it could detract from a user's experience on a website. However, many website operators are taking this approach to obtaining informed consent from their users.

- Terms & Conditions: According to the ICO, simply including the necessary information on cookies in a website's terms and conditions will not amount to prior informed consent. Acceptance of a website's terms and conditions may equal informed consent if the acceptance is achieved by a user actively consenting, such as through completing a tick box. Care should be taken in drafting terms and conditions to ensure that they include the necessary information for cookie consent.
- Implied Consent: The ICO has indicated that implied consent is an acceptable method for obtaining consent for cookies in certain circumstances. To rely on implied consent a website operator should be able to satisfy itself that a user understands that by requesting certain services, cookies may be set on their device. As such, a website operator should provide clear information as to the cookies that will be set once a user accesses such service. Commentators have questioned how implied consent will work in practice and whether the use of implied consent is in line with the EU's interpretation of consent contained in the E-Privacy Directive.

Enforcement of the UK Regulations

The ICO is responsible for the monitoring and enforcement of the UK Regulations. The ICO's potential enforcement methods range from serving information notices on non-complying website operators, to serving a binding enforcement notice compelling a website operator to follow the instructions contained therein and imposing fines of up to £500,000.

Now that the 12 month lead-in period is over, the ICO's moratorium on enforcing the UK Regulations has also ended. The ICO has stated that it will consider complaints about cookies in line with its normal approach to complaint handling. This will involve, in most cases, initially contacting the organisation responsible for setting the cookies and asking them to respond to the complaint and explain what steps they have taken to comply with the rules, prior to moving on to taking more serious enforcement action if required.

Implementation of the E-Privacy Directive in Other EU Countries

The deadline for implementation of the E-Privacy Directive was initially 26 May 2011. The UK was only one of a handful of EU member countries, if not the only one, to meet this deadline. As of April 2012 only six member states, including France, Spain and Denmark, have completed the implementation of the E-Privacy Directive into national law.

Implementation of the E-Privacy Directive into national law may vary slightly among EU countries. Consequently a company operating in more then one EU country should review the national law in each country to assure it is in full compliance with its obligations under the law.

Trainee solicitor Lauren Horman contributed to the creation of this eUpdate.