Portfolio Media. Inc. | 860 Broadway, 6th Floor | New York, NY 10003 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Time For A UK Cookie Audit

Law360, New York (June 05, 2012, 1:28 PM ET) -- Consent is now needed for most uses of cookies by U.K.-based websites.

The law, adopted in May 2011 to implement a European directive, was accommodated by the announcement of a 12-month moratorium on enforcement. Simultaneously with the expiry of the moratorium, the data protection regulator, the Information Commissioner's Office (ICO), has issued revised guidance and has invited Web users to inform it of websites that are not yet compliant.

Since May 2011, website operators throughout Europe have been required to obtain consent in relation to most cookies placed on a user's PC (or mobile device) by websites. In recognition of the challenges in moving to a consent regime, the ICO announced the moratorium. (Other countries were simply late in implementing the law change; some have not yet done so.) As this grace period has now come to an end, the commissioner will be able to look at the impact of any breaches of privacy and other rights of website users in determining whether to take enforcement action. The ICO has announced that it has already written to a number of large organizations.

Background

Prior to this change, websites only had to tell users how they used cookies and that they could "opt out," usually providing such information in a privacy policy. Now, however, a website can only put cookies on a user's device if the user has given his or her prior consent. The consent needs to be "informed"; meaning that sufficiently clear notices have to be given before the consent. The one exception to these rules is if the website's use of the cookie is "strictly necessary" for a service requested by a user.

The new rules — required by a European directive — are implemented in the U.K. by means of an amendment to the Privacy and Electronic Communications Regulations 2003 (the PEC Regs). Initial guidance on these rules from the ICO has now been revised.

The International Chamber of Commerce has also issued guidance, which many website operators will find useful.

What Is a Cookie?

A cookie is a small file downloaded onto a user's device when the user accesses a website, which then allows the website to recognize the user's device. Cookies are used for a variety of purposes such as remembering the user's name (to display when the user visits the website) or remembering the date of a user's last visit.

What Do Businesses Need to Do?

Organizations should now take the following three steps:

- Check what type of cookies and similar technologies are used and how they are used. Businesses should analyze which cookies are used. Many may be redundant and could be dispensed with.

- Assess the intrusiveness of the cookies' use. The more intrusive the use of a cookie is, the more likely it is that it will need to change. ICO advice is that more information and detailed choices will need to be provided to users for more intrusive cookies — for example, cookies that create detailed profiles of an individual's browsing activity.

- Decide the best solution for obtaining consent. There are a number of solutions, some of which are discussed in the ICO guidance (summarized below). Businesses need to bear in mind that consent does not need to be obtained repeatedly for the same person each time the same cookie is used (for the same purpose) in the future.

Potential Solutions

Express "Opt-In" Through Pop-Ups and Similar Techniques

Well-designed pop-ups are now being used by many sites to inform users of the choices. They need (to fully comply) to appear on the landing page. They also need to be clear as to what consent is actually being obtained (and often will contain a link to a cookie notice or privacy policy). A fear that this type of solution might lead to the ruin of a pleasant website experience seems perhaps to have been misconceived. The ICO themselves operated this solution soon after the law changed in May 2011.

Implied Consent

The ICO guidance has evolved since May 2011. The latest version (version 3 of May 2012) now contains a greater emphasis on when it may be possible to get "implied" consent; that is, treating the continuing browsing on a website by a user (when there is a prominent enough notice) as that user consenting to the cookies that are then served. This may be suitable when the cookies are not particularly intrusive; and a user must still know that a cookie will be served. Information provided needs to be suitable for the audience.

Terms and Conditions

It may be possible to obtain consent through terms and conditions (such as may be agreed to by users when registering on a website). A business would need to make existing users (who have already registered under old terms) aware of the changes in those terms and that they concern the use of cookies. Again, the more intrusive a cookie, the greater attention should be drawn to them.

Settings-Led Consent

It may be possible to obtain consent through the process by which users confirm what they want to do or how they want the site to work, for example, where users indicate which language version of a site they want to access or if the website should remember log-in details. (For example, "Would you like us to remember this preference? We use cookies to do so.")

Functional Uses

Collecting information about how people use a site — for example, which pages they visit on a website — still requires consent. (A common technique uses "analytics" cookies, sometimes supplied by a Google tool.) The ICO suggests a solution of footer/header text that becomes highlighted when a cookie is going to be set. This seems to be the approach the ICO has adopted for its own website.

Browser Settings

In the lead up to the new legislation, there had been much discussion of browser settings and whether they will be sufficient to indicate consent by only allowing certain types of cookies. The new PEC Regs recognized that browser settings can in some circumstances be used. However, the ICO's and the government's view was (and remains) that the functionality available through current browsers is not sophisticated enough for businesses to assume consent has been given. The U.K. government is separately working with browser manufacturers (Microsoft, Google, Apple) to change that position. In the meantime, the ICO is therefore currently advising that consent is obtained in other ways.

Third-Party Cookies

A third-party cookie is one that a website sets (or allows to be set) on behalf of another business. They are commonly used in online behavioral advertising (OBA) activities. The ICO's view on third-party cookies is that "everyone has a part to play in making sure that the user is aware of what is being collected and by whom." If a business uses or allows third-party cookies it should do everything it can to help users make informed choices.

Enforcement

There is going to be a phased approach to implementation of the changes. The ICO has stated that if it receives a complaint about a particular website, it would expect an organization to explain how it had considered the new rules and to show that it had a realistic plan to achieve compliance.

Conclusion

Businesses have had one year to get their cookies policies and procedures in order. Some will not yet have started doing so. A first step is to take stock of what cookies are being used and how intrusive they are. Once this "cookie audit" is complete, businesses can start to think about the best ways to get consent for different uses of cookies.

--By Renzo Marchini and Kate Tebbutt, Dechert LLP

Renzo Marchini is counsel and Kate Tebbutt is an associate in Dechert's intellectual property practice in London.