LEWIS SILKIN

The new UK regime for Cookies:

a guide for website owners and their suppliers

Inside

Introduction

From 26 May 2011, the UK has introduced revised rules which will require website owners to rethink how they obtain the consent of their users to cookies. In particular, the rules have been changed to remove the previous rule that users were given a right to refuse the use of cookies. The Information Commissioner's Office ("ICO"), which is in charge of enforcement, has announced a 12 month grace period (the Grace Period) during which the new rules will not be enforced, but website owners must take appropriate steps now to be fully compliant by May 2012.

Background

The UK law on cookies has been changed as a result of revisions made at European level to the EU E-Privacy Directive (the "Directive"). It requires EU Member States to amend their laws so that companies operating a website may only use cookies if each user of that website:

a) is provided with clear and comprehensive information regarding the purposes of those cookies

b) has given his or her consent

The "transparency" requirement in (a) is not new, having been in place under UK law since 2003 in response to a previous version of the Directive.

However, the consent requirement in (b) is new, replacing the previous requirement that users simply be "given the opportunity to refuse" cookies, i.e. to opt out. Because of the new emphasis on consent, the obligation to provide clear information (as in (a) above) will come under greater scrutiny by the Regulators – for his/her consent to be valid, the user must know in clear terms what he/she is consenting to.

Europe

It is important to note that many other EU Member States are still in the process of implementing the Directive into their local laws, and may adopt a different approach to the UK. The UK government is advocating the use of browser settings to indicate consent, whereas other European regulators have been critical of the adequacy of that method. The position in each European country will therefore need to be considered separately as local regulations and guidance issued by national regulators is rolled out.

The UK Government and Regulator approach to implementation and enforcement

A number of important policy statements and pieces of guidance were issued in the UK in the lead up to implementation of the new rules. Unfortunately, the guidance and policy statements issued by the Department for Culture, Media and Sport have not always been consistent with the guidance issued by the ICO.

First, a policy statement issued by the DCMS in April 2011 (the "DCMS Policy Statement") indicated that it expected companies to be able to rely on users' browser settings to decide whether consent had been given. However, recognising that browser technology is not yet sophisticated enough to differentiate between different types of cookies, the government also announced that there would be a "phased approach" to the implementation of the new law.

The ICO – which has responsibility for enforcing the Regulations – subsequently issued guidance on 9 May about the changes. The Guidance is available here.

The key points of the guidance were:

- The ICO adopted a harder line than the DCMS Policy Statement, and – while recognising that work needed to be done to improve browser technology – suggested that companies should look to other means of obtaining consent in the meantime.
- Worryingly, the Guidance also stated that website owners could not assume that all users would be accessing a website with the benefit of any new browser technology when this became available. Given this statement, it is difficult to see how browser based consent can be used to comply with the new rules – at least until the widespread roll out of new browser technology.
- An obligation on website owners to have in place a "realistic plan to achieve compliance" (a "Compliance Plan"), and suggestions of practical steps to implement such a plan which we discuss in more detail below.

The DCMS then issued an open letter, on 22 May. The open letter argued that:

- the Regulations require users to give informed consent rather than prior consent for the setting of cookies; while the natural meaning of "consent" may not usually include permission being given after the relevant activity has commenced, in the regulatory context it may be necessary to recognise that in some circumstances it is impracticable to obtain consent prior to processing

- the wording of the Regulations will (when the technology is available) allow users to indicate their consent not only by amending or setting the controls on their browser, but also by deliberately leaving their browser settings as they already are

The ICO then issued further guidance on 25 May which confirmed that it will not take enforcement action against website owners who fail to comply with the new rules during the Grace Period. However, the ICO emphasises that it does not condone organisations taking no action to prepare their Compliance Plan during the Grace Period, and it reserves the right to issue warnings to such organisations which may count against them in any post-May 2012 enforcement action. If the ICO receives complaints about a particular organisation which appears to be non-compliant during the Grace Period it may issue advice or ask the organisation to explain the steps that it is taking to ensure compliance.

The ICO's suggested practical steps

The ICO is advising website owners to take the following three steps in formulating a Compliance Plan during the Grace Period:

- Investigate what cookies are currently used on their website(s) and for what purposes. This will also enable the identification of the limited type of cookies that are excluded from the new transparency and consent rules
- Assess how intrusive each of these cookies is, in terms of the privacy impact they have on users. For example, cookies used for the purposes of behavioural advertising and building up a profile of a user across a number of websites will have a greater privacy impact than session cookies or analytics cookies. Note that the ICO suggests that the more intrusive cookies should be prioritised when considering how to obtain consent
- Decide on a solution to obtain consent for the use of cookies

Non-browser based Consent?

The ICO Guidance - pending the roll out of new browser technology - contains a list of other means of obtaining consent, depending on the particular types of cookies used:

- Pop-ups or splash pages, though the ICO recognises the disruptive effect these can have on a user's website experience
- Accepting terms and conditions that contain a user's consent, provided of course that the provisions regarding cookies are brought to a user's attention and not hidden in small print
- Settings-led consent, where a user is presented with information about a cookie when changing a particular setting on a website (such as preferred language)
- Feature-led consent, where a cookie is deployed upon activation of a particular feature of a website, such as embedded video. Again, because the cookie relates to a particular and discrete aspect of the website rather than the whole site generally, it is easier to seek consent on a less disruptive basis

In practice, it is likely that a website of even a minimum level of sophistication will need to employ one or more of these means to obtain consent to use each type of cookie.

There is enough information contained within the ICO Guidance for website owners to commence formulating a compliance solution. For example, the simplest solution would be for the website owner to require users to indicate consent to their website Terms and Conditions (which would contain detailed information about the use of cookies) on the landing page of the website.

However, that approach would require users to either accept or decline the use of cookies in general rather than consenting to (or not consenting to) particular types of cookies, meaning an 'all or nothing' response. Those users that decline consent would not be able to use the website. This rather blunt approach is therefore not very appealing.

What should website owners do now?

Given the Grace Period being offered by the ICO, we do not believe that there is any advantage for website owners to fast-track a compliance solution. Amendments should not be made to a website's current Terms and Conditions or Privacy Policy or any other aspect of a website until website owners have been able to consider the ICO's Guidance in the context of the full range of cookies used on their sites. The ICO has expressly said that it will not take enforcement action against website owners where they can demonstrate that they are implementing a Compliance Plan.

We suggest that the initial stages of the Grace Period are used to undertake a detailed audit (on a website by website basis) of the use of cookies, focusing on the following questions:

- What cookies are used on the website?
- For what purpose is each cookie, or category of cookie, used?
- Of these cookies, are any strictly necessary for the website to function or are any of these cookies strictly necessary for a service explicitly requested by the user (for which the Regulations do not require consent)? In the context of a non-trading website, this might extend to requests by users to be added to email distribution lists, or to enter prize competitions
- What information is collected by each cookie, or category of cookie?
- Is any information which is collected by the use of cookies shared with third parties?
- Do any cookies placed via the website record information about a user's visit to third party websites?
- Are any of the cookies used by the website no longer relevant or necessary (for example, if they have been superseded by other cookies or by the features of the website)?
- Of the remainder, is it possible to define these cookies into categories (for the purposes of deciding on a best-fit compliance solution for each category)?

Once answers to the above questions are in hand, it will then be possible to develop - and put in place by May 2012 at the latest - a compliance solution that identifies the various types of cookies used, explains the role of those cookies to the user and obtains an appropriate means of consent for each. This will certainly require amendment to a website's Terms and Conditions and Privacy Policy, though it could also require that other methods of obtaining consent are used such as pop-ups, on screen text (in website headers or footers) and/or splash pages.

Issues for suppliers

Finally, the above describes a website owner's statutory compliance obligations regarding the implementation of the new law. However, where a website owner has engaged a supplier to provide services where those services involve the development, management or support of a website (a "Supplier"), then the Supplier may be under a contractual obligation (i) not to act or omit to act in a way that places the website owner in breach of the law; and/or (ii) to comply with applicable data protection and/or general law. In such circumstances the approach described above (putting in place a Compliance Plan during the Grace Period) will not avoid the Supplier being in breach of such obligations as the new law comes into force on 26 May 2011. Suppliers should therefore check their agreements to ascertain whether a failure by them or the website owner to implement the new law as of 26 May could result in contractual liability to their client.

For further information on this subject please contact:

Simon Morrissey
Partner
T + 44 (0) 20 7074 8221
simon.morrissey@lewissilkin.com

LEWIS SILKIN

5 Chancery Lane – Clifford's Inn
London EC4A 1BL
DX 182 Chancery Lane
T +44 (0)20 7074 8000 | **F** +44 (0)20 7864 1200
www.lewissilkin.com