

Cookies: the rules become clearer

Businesses and other website operators looking for a belated new year's resolution should take a look at the [revised guidance on the use of cookies](#) (PDF) issued by the Information Commissioner's office just before Christmas and start thinking about how to comply.

Launching the guidance, the Information Commissioner said that businesses "must try harder" in preparing to comply with the new law, which came into force in May 2011 and will be fully enforced from the end of May 2012. More constructively, the revised guidance sets out some practical measures which websites can adopt to help ensure compliance with the new law.

The new law requires websites to obtain prior, informed consent from users before placing cookies on those users' computers or mobile devices. As the new guidance puts it, before setting cookies you must:

- tell people that the cookies are there;
- explain what the cookies are doing; and
- obtain their consent to store a cookie on their device.

The only exception is where the cookie is "strictly necessary" for technical reasons. The guidance confirms that this is a narrow exception, and will not (for example) cover cookies used for analytics or to tailor a greeting when a user returns to a site.

As a start point for compliance, the ICO guidance recommends a three-step approach:

1. Check what type of cookies you use and how you use them
2. Assess how privacy-intrusive your use of cookies is
3. Decide how to obtain consent from users

The more privacy-intrusive your use of cookies is, the more you will need to do in order to inform users and get their consent.

Providing information

The ICO recommends that cookie information should not simply be hidden behind a link saying "Privacy

policy". Instead, links should either read "Privacy and cookies", say, or there should be a separate link for information on cookies. The guidance gives several examples of how to make this information more prominent.

Inferring consent

One very helpful suggestion made by the ICO is that consent to placing could be inferred if a user continues to use a website after being told of the use of cookies. This would involve some kind of pop-up notification when the user first visits the site, with a confirmation that a cookie has been set if the user then continues on to another page without clicking the "refuse cookies" link.

I suspect that this approach will prove highly popular with websites, given it avoids the problem experienced by websites that require positive consent such as ticking a box before placing cookies. One analysis suggested that only around 5% of users of the ICO's website (which follows this tick-box approach) were agreeing to cookies – a figure which would have been ruinous for many websites.

However, inferring consent does still require a clear message to be displayed to first-time visitors. It is not enough to rely on a general "Privacy and cookies"-type link.

Opportunities for consent

The ICO guidance also suggests that websites look out for opportunities to obtain positive consent from users. One opportunity comes where new registered users are asked to agree to its terms and conditions as part of the sign-up process – though existing registered users will need to be told about any change to the terms to allow for cookies.

Other opportunities may come where users set preferences or use new features for the first time: for example, a notice saying "We will use a cookie to remember this", with a link to the cookies policy.

Analytics cookies

Analytics cookies – often for Google Analytics – are one of the most widespread types of cookie. The ICO’s position on analytics cookies is that they are not technically essential for websites, so consent will be required for them.

The ICO recognises that in some cases it is not practical to obtain consent before setting analytics cookies, as these are often set the moment a user first visits the site. However, in that case information on the use of cookies must be highlighted clearly on the site.

Having said all that, the ICO does drop a large hint that it does not regard analytics cookies as posing a serious risk to privacy. In the very last paragraph of the 27-page guidance document, they state that “it is highly unlikely that priority would be given to focusing on uses of cookies where there is a low level of intrusiveness” – which includes “first party cookies used only for analytical purposes”, provided clear information is given on the site.

Third party and advertising cookies

Third party cookies, especially those used for online advertising, are the most problematic from a privacy point of view. The ICO’s research suggests that even well-informed internet users are unaware of the distinction between first party and third party cookies – that is, cookies used by someone other than the website owner.

Information on the use of third party cookies will need to be clearly set out as part of informing users and obtaining consent. Both the website owner and the third party will want to ensure that their respective obligations are clear: if you run an advertising-supported website, you will want to ensure that the advertising provider is obliged to provide accurate and complete information on their use of cookies (so that you can put this in your own cookies information); conversely, the advertising provider will want to ensure that participating websites are compliant with the law, as otherwise this will put the advertising provider themselves in breach.

The guidance acknowledges, though, that third party cookies remain “one of the most challenging areas in which to achieve compliance”, given the higher privacy concerns over such cookies and their critical importance to online advertising.

Conclusion

It remains to be seen how the new law will operate in practice. Levels of compliance remain woefully low, so it is hard to discern any “best practice” emerging at present. However, the ICO’s guidance does at last suggest some practical ways in which websites can comply with the law without losing the benefits of using cookies.

For more information please contact:



John Halton

Partner

T: +44 (0)1892 506 351

E: john.halton@crippslaw.com