SQUIRE SANDERS

"COOKIES" DIRECTIVE - TAKE ACTION TODAY!

May 2011

Does your business operate an interactive website aimed at UK consumers? If so, changes coming into force on Thursday 26th May 2011 will affect your business and to avoid sanctions from the Information Commissioner's Office (ICO) you need to start taking action now. This alert focuses on the UK but a similar change in applicable e-privacy laws is being implemented across the European Union and in some countries may involve even greater limitations going forward.

What is changing?

Current legislation requires website operators to inform users about the fact that cookies are being used and provide guidance on how these may be disabled. The majority of website operators have in the past complied with this by setting out this information in privacy policies or website terms of use.

However, the revised "Cookies" Directive (2002/58/EC) will require website operators to take a more active role to ensure that users are informed and provide their consent to the use of cookies stored on their devices (including for instance laptops, desktops and mobile devices).

The ICO has recently published guidance for businesses to assist in their compliance with the UK Regulations implementing the Directive. Additional guidance has also been issued by the Department of Culture, Media and Sport (DCMS) in an open letter dated 24 May 2011.

What are cookies?

Cookies are small text files that are stored on a user's device when visiting a website. The cookie assists the website in recognising the user's device, for instance in order to deliver a more tailored and user-friendly experience to the user. Cookies may also be stored on a user's device by third parties who may use them to tailor their content to that particular user (this technique is often used in the context of online behavioural advertising (OBA)).

What do you need to do now?

Businesses should take the following immediate actions:

1. Review the cookies and similar technologies (such as flash cookies, browser cookies, etc) currently used on your website, including any third party cookies used by advertisers or advertising brokers, to assess which ones are strictly necessary to provide users with the web-based service and those which are not. This review should result in anything from a complete website audit through to a review of specific data files currently placed on users' devices.

2. Consider how intrusive these cookies are and talk to third party cookie providers to agree a suitable approach. The ICO has stated that "The more privacy intrusive your activity, the more priority you will need to give to getting meaningful consent".

3. Begin to create and implement appropriate and tailored solutions to gain users' consent.

What happens if you get it wrong or don't do anything?

Under the new Regulations the ICO now has the power to impose monetary penalties of up to £500,000 where serious breaches of the Regulations have been committed.

Whilst the government has indicated that there would be a "phased approach" to the implementation of the new regime, from 26 May the ICO will expect all businesses to have reviewed their cookies practices and to have a practical and effective strategy in place to obtain users' consent. In a guidance note released on 25th May, the ICO however indicated that it would generally not look to take formal enforcement action before May 2012, which should allow some time for organisations to decide on their compliance strategy.

How do you obtain consent?

Can you just use Browser settings?

The government is consulting with key browser manufacturers to see if this approach will be appropriate in the future. However, the ICO's current view is that the majority of browsers will not have the level of sophistication required to reliably obtain user consent.

What other options are there?

Except in limited circumstances (detailed below), the ICO recommends that consent should be obtained before a cookie is initially set on a user's device. Provided the same cookie is used for the same purpose, consent does not need to be obtained each time that cookie is used. The ICO has provided some guidance on a range of methods available for obtaining consent, these include:

- Pop ups and similar techniques

  Using a pop up is a clear way of obtaining express consent from the user. However, this is likely to be disruptive for a user's experience if numerous cookies are being used and many online operators have already indicated that this option is unlikely to be very practical.

- Terms and conditions

  Consent could be obtained through changes to website terms of use that would reflect the new regime. However, these changes must not only be brought to the user's attention but should also be understood and agreed by users before cookies are set on their device. Users would need to actively show their acceptance by, for instance, ticking an "accept" box, which brings this technique for obtaining consent close to a "pop up".

- Settings-led and feature-led consent

  Users can choose certain settings to set their preferences (e.g. personalised greeting or language choice) or personalise the subject matter that the user receives (e.g. by, for example, remembering the user's history). Website operators could ask the user whether they would like the website to remember these settings/preferences each time they visit, reminding them that their consent to this would only have to be given once. Users could also indicate their consent when the link is opened or when agreeing to the functionality being switched on.

- Functional uses

  Cookies which are beneficial to the website operators, by recording certain information (e.g. how often certain pages are visited by a specific user), will require consent. Such practice should be explained to the user, with further details made available. The ICO has suggested that one way of doing this would be to include information in the header or footer of the page which, when highlighted, brings up additional text prompting the user to read further and make relevant choices.

It is interesting to note that, for the time being, the ICO has decided to use a layered information notice (as a 'header' on its website at www.ico.gov.uk), incorporating a link to its privacy policy (which details the various types of cookies used by the site) and a consent box for users to agree to the use of cookies through the site.

Are there any exceptions?

The ICO indicates that there is one exception to the requirement to obtain consent. This is where the website is using a cookie that is "strictly necessary" to perform a service and that service has been explicitly requested by the user. This is a narrow exception but the ICO anticipates that this would cover, for instance, the situation where a website user adds goods to a virtual basket. The cookie or relevant functionality would retain this information to "remember" items placed in the basket through to the checkout page. This type of cookie does not require express consent from the user.

What about third party cookies?

Websites may display third party content, for example advertisements, video links or even credit card payment screens, which can allow third parties to write their own cookies onto a user's device. Such cookies are often used by third parties in the context of OBA. OBA essentially works by placing a tracking cookie in a user's web browser when they visit a website displaying one of their adverts. The user can then be tracked across any website showing their adverts and can be shown adverts based on those recent site visits.

The ICO has stated that if cookies are written onto a user's device from a third party, website operators should ensure that they are doing "everything they can" to explicitly inform users that their information is being passed on. Therefore, operators should contact any third party partners and review their current contractual arrangements to decide on the best way forward in the circumstances.

The Internet Advertising Bureau (IAB) has launched a Self Regulatory Framework which proposes a privacy icon and Good Practice Principles (i.e. self-regulatory guidelines for companies collecting and using data for OBA purposes). By clicking on the privacy icon users would obtain further information about how their information is tracked and would have the ability to manage information preferences or stop receiving behavioural advertising.

This framework is the advertising industry's attempt to respond specifically to the new requirements of the amended Directive by promoting greater transparency and user control over third party cookies. The initiative has received support from the UK Government and the EU Commission. In its recent guidance, the ICO also seems to be broadly supportive of this type of scheme, indicating that these initiatives will "no doubt adapt to achieve compliance with the new rule".

How can Squire Sanders help?

To assist businesses in taking the necessary steps to comply with the new Regulations, the guide attached to this article identifies the most common types of cookies and determines how intrusive these are likely to be to users. It also examines the level of risk associated with each. We have specialists in the UK and across the European Union who can help you with your compliance strategy including to:

- Advise you on the steps you need to take in informing users about cookies and obtaining their consent;
- Draft wording for incorporation onto your websites, in privacy policies/terms of use and at the point you collect data/set cookies to demonstrate clear consent;
- Draft wording for incorporation in contracts with third party cookies providers.

For further information and advice, please contact:

Caroline Egan
Consultant, Birmingham
T: +44 121 222 3386
E: caroline.egan@squiresanders.com

Ann LaFrance
Partner, London
T +44 207 655 1752
E ann.lafrance@squiresanders.com

A Guide To Common Types Of Cookies

Type of Cookie	Details and Functions	Level of Risk (In Decreasing Order)
Third party cookies	If a webpage has third party content then the third party will be able to store cookies on the device. This will allow them to track users across multiple websites. This approach is commonly used in Online Behavioural Advertising (OBA), using information gained about users' browsing habits to allow targeted marketing based on their interests.	High risk as users' online activity is shared with a third party, often without their knowledge. Clearly, going forward if users are unaware/ have not accepted for such cookies to be stored on their device, this practice will no longer be acceptable without steps being taken to inform users and seek their consent.
Analytical cookies	Cookies used purely for the website owner's benefit, e.g. to determine how users navigated through a site, or how often users visited the site.	There is a tracking element here which may result in a higher risk. It is also done without the knowledge of the user and provides them with no direct benefit.
Cookies that allow recommendations based on user activity	For example when a user buys or views an item, the website can suggest similar products that could be of interest. Examples include Amazon recommending products you may be interested in, or YouTube using what you have viewed previously to suggest new clips.	There is a tracking element here which may result in a higher risk but it is convenient for users.
Cookies that save preferences	Websites often have a way for users to tailor how the website appears – for example, text size, language, search preferences, or whether it remembers usernames and passwords.	Lower risk due to low intrusiveness, convenience to user and an element of opt-in to that functionality which is generally activated by the user itself.
Functions where cookies are "strictly necessary"	Where the user requests a specific service and that service requires the use of cookies, e.g. implementing shopping baskets on transactional websites.	Low risk – ICO guidelines list this as an exception to the need to obtain consent.