

## World Data Protection Report

International Information for International Businesses

Monthly news and analysis of data protection and privacy issues from around the world

Volume 12, Number 1

January 2012

### The UK ICO's Updated Guidance On The New Cookie Regime: There's Work To Be Done

*By Rohan Massey, of McDermott Will & Emery UK LLP, London.*

On May 25, 2011, the amendments to the European Union's Privacy and Electronic Communications Directive (2002/58/EC), introduced by the so-called Cookie Directive (2009/136/EC), came into force in the United Kingdom. The Information Commissioner's Office (ICO), the UK regulator, published some initial guidance at the time of implementation, but noted it would follow up as required (*see analysis at W DPR, May 2011, page 9*).

On December 13, 2011, the ICO duly published an updated guidance paper reporting on the state of progress regarding implementation and offering illustrative tips on compliance.

#### New EU Cookie Regime

Prior to the implementation of the new regime by the Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2011, the position under English law, reflecting the requirements of the un-amended e-Privacy Directive, was that the provider must provide clear and comprehensive information about any cookies being used and provide the option for individuals to opt out of the cookie being used or stored on their equipment. The revised position is that (subject to limited exceptions) consent must be obtained in order to store a cookie on an individual's equipment.

Recognising that the change gives rise to compliance

concerns, in May 2011 the ICO granted a 12-month grace period for those using cookies to comply with the new legislation.

#### Key Issues

The ICO highlights a number of key areas for attention:

- notification that cookies are used;
- clear communication detailing the purpose of cookies; and
- obtaining consent to store the cookie.

The ICO believes that, although there has been progress made regarding compliance since the new regime came into force, there remains much work to be done both to raise consumer awareness regarding the use of cookies and to achieve compliance.

The updated guidance sets out some practical steps to be considered in a compliance review.

#### Identification of Cookies

The guidance suggests operators should take an audit of the cookies used on their websites. Any unused or out-of-date cookies should be deleted. The active cookies should then be grouped into those that are necessary for the service and those that are not.

## Notification of Cookie Use

Under the 2011 Regulations, unless a cookie is *strictly necessary* for the provision of a service, there is a requirement for the operator wanting to place a cookie on a user's equipment to provide the user or subscriber with information regarding the cookie. The guidance makes clear that, in this regard, *strictly necessary* is construed very narrowly.

The ICO states that a cookie allowing a shopping basket to be “remembered” as a user moves from page to page as part of an online shopping experience would be deemed necessary. Similarly, in some instances, a cookie used for resource or capacity planning for the general operation of a website, *i.e.*, to allow workload to be spread across servers, would also be deemed *strictly necessary*, and would not require consent.

However, were such cookies also to be used for advertising or marketing purposes, or to remember and tailor the website for returning users, then such uses would not be deemed *strictly necessary* and would be subject to the consent requirement.

Where a cookie is used to ensure compliance with other legislation, including the security requirements of the seventh principle of the Data Protection Act 1998, then such use would also be seen as *strictly necessary*.

Where the Regulations require information on the use of cookies to be provided to the user or subscriber, then such information must be provided in a clear, comprehensive and easily accessible format. The information given should be sufficiently detailed to enable the user or subscriber to be able to give consent for the use of cookies and to understand the consequences of not providing consent.

## Informed Consent

There has been much debate over what is required to obtain consent and when such consent must be obtained. Critically, in order for users to be able to give consent, they must be aware of what they are consenting to. This means that users need to be made aware of what cookies are and how they function. It is reported that, in early 2011, a survey of internet users found that only 13 percent of respondents fully understood cookies and how they work; 37 percent had heard of cookies but did not understand them; and 2 percent had not even heard of cookies. On this basis, it would be very difficult to see how any of the latter two groups could give consent to the use of cookies.

The Regulations require that the subscriber (the person paying the bill), or the user, consent to the placing of the cookies on his or her equipment. As set out in the Data Protection Act 1998, consent must involve some form of communication where the individual actively indicates acceptance, having been given specific and informed information. Such indication can include clicking an icon, checking a box, sending an e-mail, or subscribing to a service, provided that the individual is aware that, by the action, the individual will be giving consent.

The guidance makes clear that, although the Regulations do not specifically refer to “prior consent”, it must be implied that consent is prior, as the use of cookies before obtaining consent would lead to compliance issues. However, as many websites currently use cookies as soon as a user accesses the site, the website must do as much as possible to provide clear, comprehensive, and readily available information to the user about the use of cookies and the user's options relating to such use.

The ICO's initial guidance made clear that there is no one-size-fits-all consent solution. There are a number of different methods that can, in theory (but not necessarily in practice), be used to obtain consent, including using clear terms and conditions on websites, highlighted click-through boxes, prominent information banners, or even browser settings. In addition, the information required for consent may vary, and where the cookies collect information that is intrusive, persistent or shared with third parties, then the greater the obligation on the party placing the cookie to bring such information to the user's attention.

The Regulations provide that a user's consent may be obtained by way of browser settings. The ICO's guidance is clear that, if the browser settings are to be relied on, then the user must have actively set his or her browser to accept cookies, and the communication requirements as to the identification and purpose of the cookies being used still need to be met. For this reason, the ICO does not think that browsers currently on the market are sufficiently sophisticated to ensure that consent has been given and to allow a website to set a cookie. The guidance also states that it will not be a defence to a charge of non-compliance to claim you were waiting for browsers to become more sophisticated!

The ICO's position is clear: As there are numerous methods that can be used to obtain consent, even if compliance was not possible in May 2011, as websites and software are updated and upgraded, compliance should become easier as mechanisms for notification and consent are incorporated into the product design.

## Consent Solutions

The critical factor in obtaining consent is that, before placing the cookie, all relevant information about the cookie is effectively communicated to the individual so that his or her consent may be obtained. The ICO sees transparency as the key to effective communication, so that the individual can clearly understand the potential consequences of allowing the cookie to be placed on his or her equipment.

In some instances, effective communication of the information regarding cookies may be achieved by the renaming of the “Privacy Policy” to the “Privacy and Cookie Policy” (ensuring that the text of the policy contains sufficient information about the use of cookies and the effects of not giving consent) and making links more prominent, either by font size or location on the web page.

Where the cookie may be used “in the background” for functional or analytical analysis of users merely browsing

a website, obtaining consent is likely to be more difficult to achieve. Unlike users logging into a website who are required to consent as part of the log-in process, the casual browser is unlikely to be aware of the use of cookies. In such instances, a link to a “Privacy and Cookie Policy” is unlikely to suffice for consent purposes, and measures should be implemented to try to obtain agreement for the use of such cookies. Consider using a splash page, pop-up or banner to convey the information with an “I accept” button or a check box. (Interestingly, the ICO states that, if the website operator uses a splash or pop-up to request consent and the user does not give the consent but then continues to use the site, then it may be possible to infer consent to the use of cookies, on the basis that the user has been made aware that use of the site may involve the setting of cookies.)

Where the information collected is provided to third parties, then this must be made absolutely clear to the user with details of the third parties’ use of such information.

### Ongoing Compliance

There is no need to repeat validation of consent on every visit, although a periodic reminder is advisable. However, where the purpose of the cookie changes after consent has been given, then details of the change will need to be communicated and new consent sought.

It must be possible for the user to withdraw consent at any time, and the mechanism for doing so, along with the consequences of such a withdrawal, should be clearly communicated to the user at the time of obtaining consent. There will be an ongoing obligation on the operator to ensure that cookies are not placed on the equipment of any user that has withdrawn consent.

### Responsibility for Compliance

Although a party operating a website and placing cookies has a responsibility for ensuring compliance, the position where a third party, such as an advertiser, is allowed to place cookies on a website is less certain. The position set out in the guidance is that, in such instances, both the third party and the website operator will be responsible for compliance. It does not matter which party obtains consent, however, as long as valid, well-informed consent is obtained. For this reason, the parties are encouraged to work together, whether on contractual terms or otherwise, to ensure that they notify the user about the cookies and obtain consent prior to any cookies being set. The ICO notes that it is continuing to work with other data protection authorities to address the complexities of achieving compliance for such third party cookies within the new regime.

The guidance also makes clear that any organisation operating a website in the United Kingdom or targeting

the United Kingdom is likely to be subject to the requirements of the Regulations, even if its website is hosted overseas. However, and to the relief of many employers, the Regulations do not apply to intranets.

### Penalties and Enforcement

The ICO is not intending to enforce the Regulations before May 2012, although it reserves the right to do so where required. The guidance makes clear that the ICO is hoping that the grace period will be used by operators to consider and implement compliance programmes.

Come May 2012, the ICO is not envisaging a wave of high profile enforcements to scare operators into compliance, but it stresses that it will use a proportionate and practical approach to ongoing enforcement, and will draw on the range of penalties available to it to enforce where necessary; these include information notices, undertakings, enforcement notices, and monetary penalty notices.

### Comment

It is clear that the ICO does not see compliance with the new cookies regime as trying to make water flow uphill. Following the practical steps outlined in the guidance should, in the ICO’s opinion, make compliance relatively easy.

However, it does still acknowledge that not all methods of obtaining consent are currently viable or indeed suit everyone. In this light, the ICO will not be implementing a wave of knee-jerk formal enforcement actions against those who are not compliant in May 2012, as long as they are trying to comply. Those wilfully avoiding compliance remain at risk.

The updated guidance is very much seen as a mid-term report which can be summed up as “could do better”. The message of the guidance is that businesses and organisations should be acting now to take stock of their use of cookies and to ensure that they have considered and implemented a suitable regime for explaining the use of cookies to users and obtaining consent going forward. With potential penalties of £500,000 (U.S.\$769,564), cookie compliance is a hot topic to which companies should be giving full attention in the first half of 2012 in order to avoid being burnt when the grace period expires.

*The ICO’s updated guidance on the new cookie regulations can be accessed on its website at <http://op.bna.com/pl.nsf/r?Open=dapn-8phsq8>.*

*The ICO’s “half-term report on cookies compliance” blog post can be accessed at <http://www.ico.gov.uk/news/blog/2011/half-term-report-on-cookies-compliance.aspx>.*

**Rohan Massey is a Partner, IPMT, McDermott Will & Emery UK LLP, London. He may be contacted at [rmassey@mwe.com](mailto:rmassey@mwe.com).**