



Update on the Regulation of Cookies

by Gareth Oldale, Solicitor

The Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2011 (the “Regulations”¹) came into force on 26 May 2011, amidst some confusion in the ICT/Telecommunications sector as to who would need to comply with the Regulations, when and how. Now that the sector has had 6 months to adjust to the Regulations, this article seeks to consider what impact the Regulations have had and how the Information Commissioner is seeking to enforce the new rules.

The new rules

The most significant impact of the Regulations is in respect of cookies and the consent which individuals must give for cookies to be used. Cookies are small text files which are downloaded (often unwittingly) onto users’ computers when visiting a website. Cookies collect and remember certain information about the website user (e.g. name, password, email address, user preferences etc.). This technology is integral to the use of many websites and is used for a number of legitimate purposes. For example, on a local authority website, cookies may be used to remember a user’s log-in details, or payment preferences to assist in the payment of Council tax online.

Prior to the enactment of the Regulations, website operators were required, under the Privacy and Electronic Communications (EC Directive) Regulations 2003 (the “2003 Regulations”), to tell people how they use cookies and how users could opt out of the use of cookies. Users had to actively decide not to allow cookies - the default position was that cookies would be allowed.

Under the new Regulations, which amend the 2003 Regulations, cookies can only be placed on users’ machines where the user has provided his or her consent. Regulation 6 of the 2003

¹ A copy of the Regulations can be found at <http://www.legislation.gov.uk/ukxi/2011/1208/contents/made>



Regulations now states that “a person shall not store or gain access to information stored in the terminal equipment of a subscriber or user unless...the subscriber or user of that terminal equipment: is provided with clear and comprehensive information about the purposes of the storage of, or access to, that information; and has given his or her consent”. As a result of this change, users are now able to decide whether or not to allow cookies on their computers before those cookies are actually used.

Who needs to comply.....?

The Information Commissioner’s Office (“ICO”) has issued some guidance² on the Regulations. Both the Regulations and the ICO guidance make clear that the Regulations will apply to any person who uses cookies.

In most cases, this will be a website owner or operator, e.g. a central Government department or local authority. However, third party cookies (i.e. cookies planted by parties other than the owner of a website) are also covered. For example, where a website owner rents out advertising space on its website and the advertiser places cookies on a user’s computer, then the user’s consent will be required. As the use of online behavioural advertising and targeted marketing increases, so too will the number of third party cookies which are placed on users’ computers. As such, privacy campaigners should take comfort that third party cookies are also covered by the Regulations, whilst website operators should also consider gaining consent for the use of third party cookies.

...and how?

On one view, requiring users’ consent to use cookies ought not create much of an additional burden on website operators and cookies companies. However, some critics have argued that the relevant technology (in particular browser settings) is currently not developed in such a way to easily allow users to provide their consent and that other ways of obtaining consent are cumbersome and will detrimentally affect the user experience of a website.

² A copy of the guidance can be found at http://www.ico.gov.uk/for_organisations/privacy_and_electronic_communications/cookie_rules_prepare.aspx



In order to address these concerns, the ICO's guidance sets out various suggestions as to how to obtain users' consent. As a starting point of principle, the ICO acknowledges that cookies can be used for a variety of purposes, some of which are very sensitive and others of which are simply used to ensure the smooth-running of a website. As such, the ICO has advised organisations that "the more privacy intrusive your activity, the more priority you will need to give to getting meaningful consent".

In the medium term, it is expected that users will be able to provide their consent by way of their internet browser settings, i.e. users will be able to select if they wish to allow cookies (and if so which types of cookies) by way of altering their browser settings. At present, the ICO considers that "most browser settings are not sophisticated enough to allow you to assume that the user has given their consent to allow your website to set a cookie". Furthermore, "not everyone who visits your site will do so using a browser". They may, for example, have used a mobile phone application. For these reasons, the ICO is advising organisations which use cookies that they have to gain consent in some other way. The Government will continue to work with browser manufacturers to improve their privacy settings so that cookie consent can be provided in this way in the future. In the meantime, however, consent should be gained in another way.

The ICO guidance sets out the following examples of how an organisation might obtain users' consent to the use of cookies:

- **Pop-ups and similar techniques**, i.e. a pop-up box appears on screen before cookies are downloaded to a user's computer. Whilst technically simple, this option might spoil the user experience if multiple cookies are used on different website pages or at different stages of an online transaction, necessitating multiple pop-ups.
- **Terms and conditions**, i.e. users are asked to confirm acceptance of the website terms and conditions before accessing or using the website, including acceptance of the use of cookies. The ICO has made clear that organisations cannot simply bury a cookie consent clause within their terms and conditions. Rather, if organisations use this option to gain consent, they must make users aware of the changes to the terms and conditions and specifically that the changes refer to the use of cookies.



Users will then need to positively indicate their consent, for example by ticking a box to indicate agreement to the use of cookies.

- **Settings-led consent**, i.e. users provide consent when customising how a website works for them (for example, users can select in which language the website is presented, or the website colour scheme). If this option is used, users should provide positive consent to the use of cookies when they confirm how they wish the website to work for them.
- **Feature-led consent**, i.e. consent is provided when a user selects to use a particular feature of a website which uses cookies, for example streaming a video clip or clicking on an advertiser's link.
- **Functional uses**, i.e. where users are directed (via a header or footer, for example) to a list of the types of cookies used and are asked to consent at that time.

By way of a practical example, new visitors to the ICO's website (www.ico.gov.uk) will be greeted by a header which reads:

"The ICO would like to use cookies to store information on your computer, to improve our website. One of the cookies we use is essential for parts of the site to operate and has already been set. You may delete and block all cookies from this site, but parts of the site will not work. To find out more about the cookies we use and how to delete them, see our privacy notice."

Users are then asked to tick a box to confirm their consent to the use of cookies.

Enforcement by the Information Commissioner

The Information Commissioner has been granted new powers to, amongst other things, impose penalties of up to £500,000 for serious breaches of the Regulations and subject organisations to an audit of their compliance with the Regulations. Notwithstanding these powers, the Information



Commissioner acknowledges³ that the new requirements will be challenging for organisations and that immediate implementation of the rule requiring consent for cookies:

- could significantly restrict the operation of internet services that users generally take for granted; and
- would be likely to cause disproportionate inconvenience both to website providers and to users.

For these reasons, the Information Commissioner has allowed a 12 month lead-in period, during which organisations may develop ways of meeting the new cookie requirements. The ICO does not expect to take enforcement action against organisations that are working to address their use of cookies but at the same time does not condone organisations taking no action during the lead-in period, which ends in May 2012. As such, if organisations are not making adequate preparations to be compliant by May 2012, the Information Commissioner may issue a warning as to the future use of his enforcement powers. Any such warnings will be taken into account should further enforcement action be required.

Comment

Organisations which rely on cookies should by now be considering how they intend to meet the requirement to obtain users' consent by May 2012. This will include the majority of public authorities, which will to some extent use cookies on their websites (for example, to enable the use of online Council tax payments or remember a user's log-in details). Organisations should bear in mind the intrusiveness of the cookies they use and respond accordingly, and should be particularly mindful if third party advertisers also use their websites.

The Information Commissioner has demonstrated with the use of his powers to issue fines for breach of the Data Protection Act that he is willing to take strong action to address privacy and data security failings. Organisations would do well to bear this in mind when considering their responses to the new rules on cookies.

³ The ICO has issued guidance on enforcing the Regulations, a copy of which can be found at http://www.ico.gov.uk/for_organisations/privacy_and_electronic_communications/new_regulations.aspx



Gareth Oldale is a solicitor in Sharpe Pritchard's Projects department. Gareth can be contacted on 020 7061 5914 or goldale@sharpepritchard.co.uk.

This note does not provide specified legal advice and should not be acted or relied upon as doing so. If you would like further information or specific advice, please contact Gareth Oldale (0207 405 4600 or goldale@sharpepritchard.co.uk)