Implementation of the 'Cookie Directive' in the UK

July 15, 2011

Implementation of the 'Cookie Directive' in the UK

The so-called "Cookie Directive" 2009/136/EC came into force on the 26 May 2011 in the UK. The Cookie Directive makes a number of amendments to the Universal Services Directive *(2002/22/EC),* the Privacy and Electronic Communications Directive *(2002/58/EC)* (the '**e-Privacy Directive'**) and the Regulation on consumer protection co-operation between national regulatory authorities *(2006/2004/EC).*

The directive is referred to as the Cookie Directive because its most significant impact is to amend the e-Privacy Directive so that users of a website must consent to cookies being placed on their computers. A cookie is a piece of text stored on a user's computer by the website operator or a third party, the purpose of which is to collect information.

Both the UK Government and the Information Commissioner's Office ('**ICO**') have recently published guidance on what changes businesses and organizations will have to make to their websites in order to comply with the amended e-Privacy Directive. The ICO has granted a 12 month grace period before it will enforce the amended e-Privacy Directive in earnest and has encouraged website operators to take swift action to ensure that their websites comply with the amended e-Privacy Directive, to avoid the risk of future penalties. The ICO may act on serious breaches brought to its attention during the grace period.

Changes to Existing Legislation

Pursuant to the e-Privacy Directive, as originally enacted, website owners were required to provide the user with information about how cookies were used on the website and how users could 'opt-out' of having cookies placed on their computer. However, the e-Privacy Directive, as amended, requires website operators to obtain the consent of website users in order to place cookies on their machines. In effect, the approach to cookies has been changed from 'opt-out' to 'opt-in'.

Article 5(3) of the amended e-Privacy Directive provides that the website user must be provided with clear and comprehensive information, in accordance with the Data Protection Directive (95/46/EC), *inter alia*, about the purposes of the processing in order to give consent. This freely given, specific and informed consent must be obtained prior to the insertion of the cookie on the user's machine.

The amended e-Privacy Directive applies to all situations in which cookies would be placed onto a computer, subject to two exemptions set out in Article 5(3). Cookies may be placed onto a computer without consent for the "sole *purpose of carrying out or facilitating the transmission of a communication over an electronic communications network*" or where the use of the cookies is "*strictly necessary in order to provide an information society service explicitly requested by the subscriber or user*". With regard to the latter, the terms "strictly necessary" are expected to be interpreted extremely narrowly. For example, where a website user clicks 'add to basket' or 'proceed to checkout' in the context of shopping online and the website uses a cookie to remember the items that the user selected on the previous page, a website operator would not be required to ask users to consent to these cookies. However, the exemption would not apply to cookies placed onto a computer in order to remember the website user's preferences and make the use of the website more 'user friendly', i.e. remembering what language they wish to view the website in, as this is not "strictly necessary".

Government Guidelines

The UK Government published its response paper to the Cookie Directive on 15 April 2011, see - 'Implementation of the Cookie Directive: UK Government Publishes Its Response Paper'. The Government's preferred approach to the amendments is to work with browser manufacturers on a solution which will use enhanced browser settings to obtain the requisite consent. The possibility of such consent is provided in Recital 66 of the Directive, which states that where it is technically possible and effective, "*the user's consent to processing may be expressed by using the appropriate settings of a browser*." This in turn will give the consumers the necessary control, particularly over the thorny issue of third party cookies, whereby third parties who advertise or stream videos on an operator's website, may set cookies onto that operator's website. Thus, the user would be required to consent to two sets of cookies.

The UK Government recognises that the amended legislation has the potential to cause uncertainty for both website operators and website users. Thus, whilst penalties are unlikely to be enforced in the interim period for failure to comply (discussed further below), website operators are encouraged to abide by the spirit of the revised Directive and "*develop best practice ahead of full implementation*." The UK Government encourages those website operators who are uncertain as to the requirements of the Directive to seek advice as to how best to implement the changes.

Methods of Compliance and Obtaining Consent

The ICO published its guidance on the amendments to the Directive on 9 May 2011 (the **'Guidance'**), see - 'UK's Information Commissioner's Office Publishes Guidance on the "Cookie Directive"'. The Guidance is intended to offer suggestions to website operators as how they should analyse and / or modify their websites, in order to comply with the Directive; it is not intended to be a prescriptive list of what website operators need to do in order to comply with the amended Directive.

Firstly, website operators should seek to have a comprehensive audit of their website, thereby analysing which cookies are placed on the computers of website users and why. The audit might reveal that an operator may stop using certain cookies, as they are not necessary for the proper functioning of the website. Pursuant to the audit, the operators should analyse what type of data each cookie is storing, adopting a sliding scale to separate privacy neutral cookies (i.e. the cookie is not storing any personal data) at one end of the scale from the most intrusive cookies at the other end of the scale. If a cookie is particularly intrusive, i.e. it creates a detailed profile of a website user's browsing activities or personal data, such as storing their credit card details, date of birth and address, then website operators should seek to prioritise obtaining consent from users for this particular cookie.

Thirdly, a website operator must choose the most suitable method of obtaining consent from its website users. The Guidance provides several options as to how website operators may obtain such consent. What is clear from the Guidance is that website operators should not seek to rely solely on internet browser settings as evidence of consent. As stated above, although Recital 66 of the Directive does state that consent may be expressed through appropriate browser settings, this is qualified, such that it may only be done if it is "*technically possible and effective*". This is because not all browsers are currently sophisticated enough to demonstrate that a user has given its consent to cookies being used and not all users will be accessing the website via a browser. For example, certain users may access the website via a mobile device. Thus, other methods, including, inter alia, obtaining consent through pop-ups, terms and conditions and settings-led consent, whereby the user agrees to having its preferences for the website adopted, are recommended by the ICO as potential solutions for obtaining consent. The appropriate method of gaining consent will depend on the nature of the cookie.

Non-Compliance

The ICO published a paper on its enhanced enforcement powers at the end of May 2011. The Information Commissioner will have discretion over how it uses its powers, within reason, as the ICO is a public body subject to judicial review. The enhanced powers will allow the Information Commissioner to impose civil penalties of up to £500,000 for a serious breach of the e-Privacy Directive. The circumstances giving rise to such a fine are: (i) a serious contravention of the e-Privacy Directive; (ii) contravention of a kind likely to cause substantial damage or distress; and (iii) if the contravention was deliberate, or the person responsible ought to have known that the contravention would occur and failed to take reasonable steps to prevent it.

The guidance on enforcement states that businesses will be given a grace period of 12 months ending in May 2012, before the ICO considers using full enforcement powers to compel businesses to comply with the amended legislation. However, the 12 month grace period does not mean that businesses can refrain from taking any action until May 2012: if the ICO is of the view that a business is not making any headway with actioning preparations, then it may either issue the business with advice on how to comply with the legislation or a warning that it may use its

enforcement powers. Likewise, the Governmental guidance states that implementation will be phased in according to a transition schedule. The phasing in of the amendments mirrors the phasing in of the Directive, when it originally came into force.

If a website user was to complain about a particular website to the ICO, the website operator in question would be required to set out a response to the ICO as to how it has considered the amended e-Privacy Directive and intends to be fully compliant in due course. An organisation not intending to change its current practices or ignoring the amended e-Privacy Directive would be noted for its failure to comply with the e-Privacy Directive.

What is not yet certain is how widely the enforcement powers will extend: will the powers apply solely to websites operated within the UK, or those that target UK customers, irrespective of where they operate from? For example, if a company has its server in the US, but it specifically targets users in the UK, by agreeing to ship goods bought on the website to the UK, it is not yet entirely clear how such websites will be affected and whether they will have to comply with the legislation. It is assumed that if the ICO publishes further guidance on enforcement, such issues would be addressed.

Data Protection

Although not explicitly covered by the Cookie Directive, the issue of data protection is one which is nonetheless worth considering, given that businesses are advised to undertake an audit of their website. The correlation between cookies and data protection was elucidated in the Article 29 Working Party Opinion 8/2010 adopted in December 2010. The Working Party is the independent EU Advisory Body on Data Protection and Privacy.

In its opinion on online behavioural advertising, the Working Party indicated that non-EU operators using cookies on users' computers that collect personal data should fall within the scope of the Data Protection Directive. This is because the Working Party reasons that the cookie collects personal data that is then processed in the EU by the users' computers. Using equipment within the EU to process personal data is one of the triggers for the Data Protection Directive to apply.

The opinion of the Working Party is an interpretation of current legislation and is likely to be indicative of explicit future amendments to the Data Protection Directive; therefore it is appropriate to consider the impact of the Working Party opinion when considering what impact cookies have on a business' website.

Conclusion

The amended Directive leaves it up to Member States as to how they implement the changes. Thus, the method of consent may be prescribed in certain jurisdictions, and may be simply recommended in others. The patchwork quilt of legislation that may arise, could result in website operators having to adopt different methods of obtaining consent from each of their website users, depending on which jurisdiction the user is located in. The Government's response paper does make it clear though that the UK regulations will mirror the requirements of the Directive, save for the ability of an internet user to change the default settings on an internet browser in order to consent to the use of cookies.

As the amendments come into force, website operators are advised to undertake a comprehensive audit of their use of cookies and consider what steps they will need to take in order to comply. Although enforcement action is not expected to be taken in the short term, all website operators still should bear in mind the risks of future enforcement and negative publicity for an ongoing failure to comply.