RUSSELL-COOKE | SOLICITORS

Cookies

Summary

UK regulations that came into force in May 2011 mean that organisations now need the consent of individual visitors to their website if they are to use “cookies”. The Information Commissioner gave a grace period of 12 months for organisations to address the regulations but they now need to consider how they intend to tackle the legal, technical and practical implications of the legislation.

What is a cookie?

Cookies are digital markers which are placed on the computer of an individual when they visit a website and allow the operator of that website to gather information about the user. In many cases they are essential to enable a website to run effectively and provide the user with an enjoyable experience but they also present privacy issues as a result of the link that is made between the website and the user’s computer.

There are different types of cookies which can perform a variety of functions.

- “Targeting” or “advertising” cookies allow organisations (and often third party advertising networks) to trace an individual’s use of the internet and the type of sites they use; information which can then be disseminated to other organisations and advertisers to assist with targeted marketing.

- “Functionality” cookies aim to give users a better service by remembering certain details about them which can then be accessed when they return to the website.

- “Performance” cookies allow an organisation to consider the effectiveness of their website and the number of visitors to particular pages.

- “Strictly necessary” cookies are those that may have to be used by the organisation to enable certain secure areas of the website to be accessed.

The different types of cookies and the ways in which they are used have different implications for how they should be dealt with in light of the requirement for a user’s consent.

Consent

The regulations require an organisation with a website to obtain the consent of the individual user to use cookies. The consent must be freely given by the individual and should be given on the back of clear and comprehensive information provided to them. The consent cannot be inferred by a user’s silence on the subject.

Just a few days before the grace period ended, however, the ICO stated that *implied* consent would be considered a valid form of consent. This means that users will not be required to expressly state they accept cookies being set (for example, by ticking a box when they first arrive at a website) but equally the ICO have warned organisations about relying on a privacy policy tucked away deep within a website. Relying on implied consent means that organisations should still be making serious efforts to direct users to clear information about the website's use of cookies if they want to be able to say the consent is informed.

The key concern for any organisation using cookies should therefore be how they provide users with the clear and comprehensive information which in turn informs their consent.

What will amount to consent to satisfy the regulations may well depend on the type of cookies being used and the way in which those cookies deposit and access information. As a general rule, the more intrusive a cookie appears to be the greater the efforts an organisation should go to so as to bring it to the attention of the user.

Cookie audit

The ICO will want to see that all organisations have made an effort to comply with the regulations or have at least started to seriously consider how they are going to do so. A good first step in the right direction for any organisation will be to carry out a "cookie audit".

This would involve checking the organisation's current website and its use of cookies first of all. A thorough analysis of whether or not all those cookies are required and how intrusive those cookies are to an individual user should then be carried out. Depending on the outcome of this analysis the third step should then be to consider whether or not to change the cookies and their use and more importantly what lengths to go to in order to obtain the consent of users.

Such an audit may well be an intensive process and will probably require organisations to draw on the knowledge and expertise of different people, both internally (IT department, marketing department) and externally (website developers, lawyers).

Compliance

The ICO has not been prepared to provide firm instructions on what organisations should be doing to ensure compliance. Different organisations will inevitably adopt different approaches and each will have to tailor their response to the regulations, their own requirements and those of their website.

Whatever the approach adopted there is clearly a balance to be struck between minimising the risk of non-compliance whilst maintaining a website that attracts users and run smoothly. Below are a number of possible solutions to consider:

- Pop-up windows – every time a user visits a new part of the website a window could pop-up to explain that the page uses cookies and ask for express consent from the user. Whilst there is likely to be little doubt that a user's consent has been obtained it raises serious issues about the functionality of a website and could be costly and a technical challenge to implement.

- Privacy and Cookies policy – A revised privacy policy which sets out in detail the website's use of cookies is probably a very good idea. Organisations may even want a separate cookies policy to highlight the issues. Equally as important as the policy itself, which should be clear and in non-technical language that the average user can understand, is where the link to the policy is placed on the website. Organisations stand a better chance of complying if the link is prominently located. An alternative is to place a clear cookies notice on the front page of the website and/or at the bottom of every other page of the website.

- Browser settings – A user's browser settings may imply permission for a website to use cookies but it is probably best not to rely solely on browser settings and, at the very least, a website's privacy policy should direct the user to reconsider their browser settings. In addition, browser settings may be appropriate for most uses of cookies but it may be more difficult to infer consent in relation to the most intrusive types of cookies (such as targeted or third party advertising cookies).

The various options all have their problems. An organisation must consider the risks of non-compliance alongside the expense and technical issues in adapting to the regulations whilst still ensuring that the website operates as they want it to and projects the desired image to users.

Looking forward

The ICO has acknowledged the difficulties in adapting to the regulations but now that the grace period has ended they are unlikely to let organisations just sit back and refuse to even attempt to comply on the basis that it will have a detrimental impact on their business. The ICO will have the power to impose heavy fines although it is expected that they are more likely to use their powers to approach organisations and query why they are not doing enough to satisfy the regulations. This may result in a demand to see a timetabled plan to move the organisation towards compliance and regular checks on the progress of such a plan.

It is impossible to know exactly how the regulations will play out but whatever their impact, it is vital that all organisations look to address the issue of cookies and consent now.

For further information please contact:

Andrew Studd
Partner
+44 (0)20 8394 6414
Andrew.Studd@russell-cooke.co.uk

Simon Ewing
Solicitor
+44 (0)20 8394 6449
Simon.Ewing@russell-cooke.co.uk

This material does not give a full statement of the law. It is intended for guidance only and is not a substitute for professional advice.
No responsibility for loss occasioned as a result of any person acting or refraining from acting can be accepted by Russell-Cooke LLP.

www.russell-cooke.co.uk