STEVENS&BOLTON

DATA PROTECTION COOKIES

BACKGROUND

The Privacy and Electronic Communications (EC Directive) Regulations 2003 ("Regulations") implemented the provisions of Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector. The Regulations have been amended several times since their introduction in 2003. The respective amendments have spanned various areas of the Regulations including the rules on marketing calls, cookies, emergency text alerts and enforcement of breaches. This note focuses on the application of the Regulations to the use of cookies on websites.

WHAT IS A "COOKIE"?

A cookie is a small, often encrypted text file downloaded onto a device by an online provider when a user accesses certain websites. Cookies collect information about the internet user which is transmitted back to the originating website on each subsequent visit. They can be useful in assisting the effective navigation of webpages.

THE LAW

On 26 May 2011 the Privacy and Electronic Communication (EC Directive) Amendment Regulations 2011 ("2011 Amendments") came into force and amended regulation 6 of the Regulations.

Regulation 6 now provides that a person must not **store or gain access to information stored** in terminal equipment (computer or mobile phone) of a **subscriber or user** unless the subscriber or user:

(a) is provided with **clear** and **comprehensive** information about the purpose of the storage or access; and

(b) has given **consent**.

The General Data Protection Regulation ("GDPR") introduced a new concept of consent. The Information Commissioner's Office ("the ICO") has confirmed that the GDPR concept of consent applies to the Regulations.

PRACTICAL POSITION

As a result of the 2011 Amendment to the Regulations any website which uses cookies must (i) provide website users or subscribers with **clear and comprehensive information** about the cookies used on the website (ii) their **purpose** and (iii) obtain **consent** to the use of the cookies unless one of the exceptions applies.

Having to get GDPR compliant consent means users will need to actively give consent. Users should also be able to withdraw consent if they wish to and this should be easy for them to do.

ENFORCEMENT

The ICO is responsible for enforcing the Regulations.

The ICO can require organisations to provide specific information via information notices or issue enforcement notices requiring specific action to be taken. Failure to comply with the Regulations can lead to criminal prosecution, non-criminal enforcement and audit. The ICO can also serve a monetary penalty notice imposing a fine of up to £500,000 for serious contravention of the Regulations.

The ICO's guidance on cookies states that it will take a risk-based approach to enforcement in this area and that particular care should be taken to ensure clear and specific consent is obtained for more privacy-intrusive cookies, such as those collecting sensitive personal data like health details, or used for behavioural tracking.

THIRD PARTY COOKIES

If third party cookies are set up through the website, both the owner and the third party who set up the cookie may be responsible under the Regulations. In practice however, complaints are likely to be made against the website owner. Therefore, website owners should consider putting contractual restrictions on third parties not to set third party cookies without the website owner's consent and should also consider imposing contractual obligations with regard to the information and consent provisions.

In order for consent to meet the GDPR's requirements, it needs to be 'specific'. This means that any third party controllers relying on the consent such as online advertisers technically would need to be named in the consent wording.

"STRICTLY NECESSARY" EXCEPTION

There is an exception to Regulation 6 if the technical storage of or access to information is used:

(a) for the sole purpose of carrying out transmission of a communication over a communications network; or

(b) where such storage or access is **strictly necessary** for the provision of an information society service **requested by** a subscriber or user.

The strictly necessary exception is met, for example, when buying a product, a cookie is used to retain the information needed to proceed to checkout from the basket. The exception is unlikely to apply to analytical cookies, advertising cookies or cookies used to recognise a returning user to a website to give a personalised greeting.

WHAT DOES THIS MEAN FOR ORGANISATIONS?

In order to achieve compliance, it may be useful to take the following steps:

Step 1 - audit cookies

First, undertake a web site audit to find out which cookies or similar technologies (if any) are used:

- Identify which cookies are operating on or through your website

- Confirm the purpose(s) of each of these cookies
- Confirm whether you can link cookies to other information held about users - such as user names
- Identify what data each cookie holds
- Confirm the type of cookie - session or persistent
- If it is a persistent cookie, how long is its lifespan?
- Is it a first or third party cookie? If it is a third party cookie, who is setting it?
- Double check that your policy provides accurate and clear information about each cookie

Step 2 - prioritise cookies

Once the organisation is aware of which cookies it is using, these can be prioritised.

- Analyse any which are **strictly necessary**
- Delete and clean up any **not used or hardly used (non-essential)**
- Can any non-essential cookies **be disabled** immediately?
- **Grade cookies** on a sliding scale from most **intrusive** to privacy neutral and focus first on the most intrusive
- Locate the most intrusive cookies which the website uses and consider if any cookies should be disabled pending consent
- The International Chamber of Commerce UK ("ICC UK") has provided categorisations of cookies as set out in step 3 below

Some examples of cookie types are:

- Session/transient (which expire after the browser is closed and are short term)
- Persistent/permanent or stored (stored longer for terms i.e. between browser sessions)
- Flash Cookies/local shared objects
- First party cookies (sent by the actual website being visited)
- Third party cookies (sent by a third party website other than the one being used by the user)

Whether a cookie is "**intrusive**" is in effect a judgment call. If the cookie has no impact and merely keeps the users' information safe, this could be graded as low. An analytical tool that shows which pages are visited frequently or which links are used may be less intrusive if the information collected cannot be linked back to an identifiable individual. However, a cookie which creates profiles of an individual's browsing habits is likely to be seen as more intrusive, as is a cookie which collects personal data. Also, cookies used as marketing tools as opposed to those used for enjoyment of the site, may be seen as more intrusive. Those which last longer may also be considered as more intrusive.

Step 3 - inform users of the cookies

Give the website user clear and comprehensive information about:

- What cookies are used on the website
- The purpose of the cookie and who it is used by

The ICC UK has also helpfully divided cookies into 4 categories; strictly necessary, performance, functionality and targeting/advertising cookies. For each type of cookie, the ICC UK suggests a description to be used to explain the cookies. In addition the information about cookies should be clear, comprehensive and prominent. It must also be easily accessible to the user. You should, therefore, consider if it is appropriate to place the details of cookies in the privacy notice or a separate cookie policy. You should also provide details at the point of consent.

STEP 4 - ENABLE USERS TO SIGNIFY CONSENT

In practical terms, it is this aspect of the Regulations which requires the greatest amount of thought. The ICO does not specify exactly how consent should be obtained. Methods for consent can include banners, tick box or clicking on an icon.

Consent obtained must meet the GDPR's requirements for consent. The GDPR requires that consent is "**freely given, specific and informed**". It must also be "an unambiguous indication" of the individual's wishes by which he or she, "by a statement or by a **clear affirmative action**", signifies his or her agreement.

As consent must be freely given, it should be possible for customers to use the website without cookies (except those falling under the strictly necessary exception) and an **easy way for users to disable** cookies should be provided.

The website operator and any other **controllers** relying on the consent **should be named** in the consent wording so that the consent is sufficiently specific and the user or subscriber can make an informed decision.

In order to ensure consent is given by a clear affirmative action, it would be safest to have a tick box or cross approach where customers **positively opt-in** to cookies. If an individual does not tick/ cross the relevant box to show their consent to cookies, it is not necessarily compliant to carry on using cookies. An individual simply continuing to use a website will likely not be considered to be an affirmative action.

Arguably, consent must be obtained **before the cookie is activated** in order for the consent to be informed. This may cause practical issues where websites contain cookies which are activated as soon as the users access the site. The ICO's advice on this point is that, where this is unavoidable, the website owner should at least reduce the amount of time between the cookie being activated and consent being given. This would mean making the information about cookies very prominent and easily accessible to the website user (e.g. by means of a pop up or a banner).

WITHDRAWING CONSENT OR CHANGES TO USE OF COOKIES

Provision should also be made for withdrawal of consent by users and the website should provide information on the consequences of this.

Users should be able to pick and choose between which cookies they consent to, for example, by being able to opt in to analytical cookies set by the website operator but not advertising cookies placed by third party controllers.

The website will also need to provide information on changes to use of cookies.

RECORDS OF CONSENTS

Website operators need to have records of the consents collected and will wish to check that their technical systems facilitate this. Third party controllers will also need to be able to demonstrate consent and so will need a right to audit and access consents.

EPRIVACY REGULATION

It is anticipated that the Regulations will be replaced by the proposed ePrivacy Regulation, though the text of the ePrivacy Regulation is still in draft form. Accordingly, further developments in this area are expected in due course.

SUMMARY

The objective of the cookies Regulations is to encourage organisations to be transparent about the information being collected from website users and how this information is being used. It also aims to educate users so they become more aware of where and how cookies are used so their privacy is respected.

Businesses now need to obtain GDPR compliant consent to cookies. Businesses should check whether the consent wording and mechanisms that they have in place are sufficient to meet the requirements of the GDPR.

KEY CONTACTS

For further information about any of the issues raised in this guide, please contact:

Beverley Flynn
Partner
T: +44 (0)1483 734264
M: +44 (0)7769 708486
E: beverley.flynn@stevens-bolton.com

Beverley Whittaker
Partner
T: +44 (0)1483 734281
M: +44 (0)7867 522929
E: beverley.whittaker@stevens-bolton.com

Charles Maurice
Managing Associate
T: +44 (0)1483 406971
M: +44 (0)7557 677192
E: charles.maurice@stevens-bolton.com

STEVENS&BOLTON

Wey House, Farnham Road
Guildford, Surrey, GU1 4YD
Tel: +44 (0)1483 302264
Fax: +44 (0)1483 302254
DX 2423 Guildford 1
www.stevens-bolton.com

\39769v6