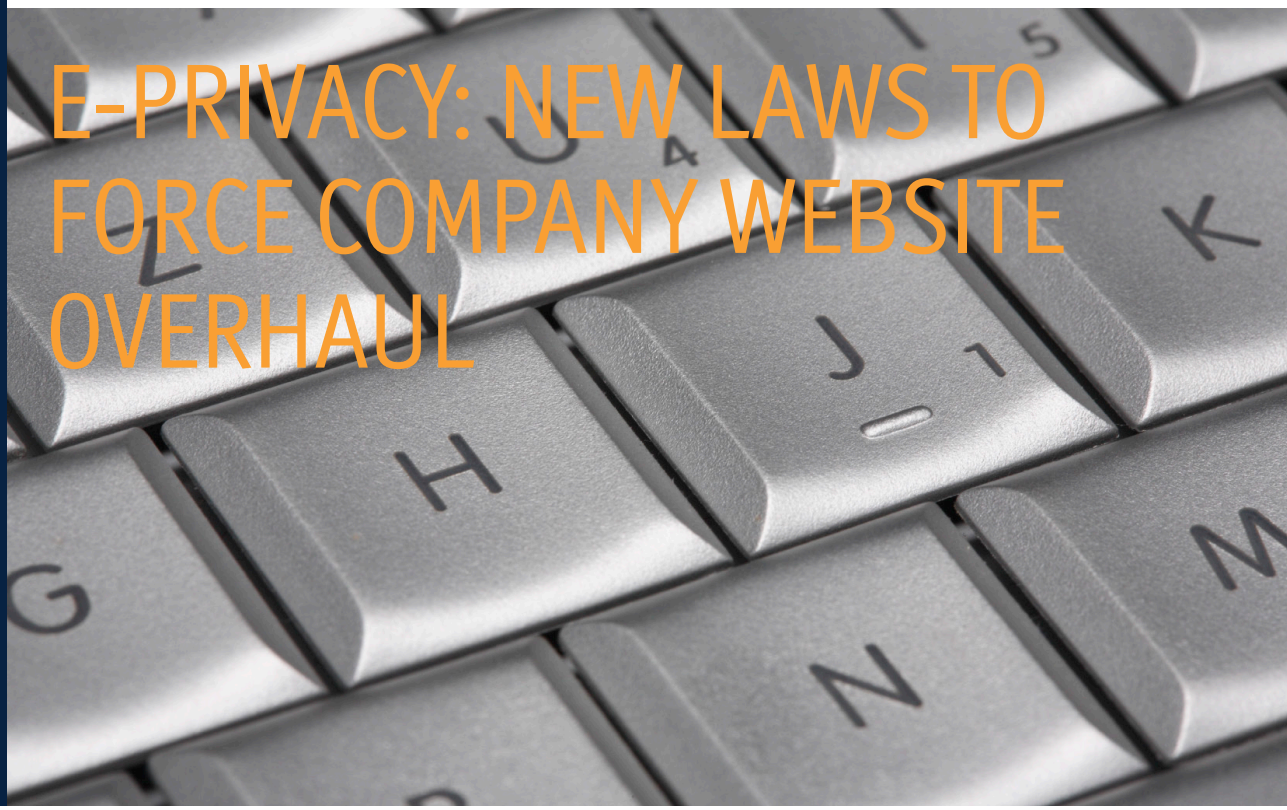
IP/IT

June 2011



E-PRIVACY: NEW LAWS TO FORCE COMPANY WEBSITE OVERHAUL

London

Paris

Rouen

Brussels

Geneva

Piraeus

Dubai

Hong Kong

Shanghai

Singapore

Melbourne

Sydney

Perth

New laws came into effect on 26 May 2011 which will have a significant bearing on UK businesses and organisations running websites in the UK.

The amended Privacy and Electronic Commerce Regulations[1] (the "amended Regulations") implement the revised E-Privacy Directive[2], which the EU adopted in December 2009 as part of a review of telecommunications and electronic communications in the EU.

The principal amendments introduced by the new legislation:

1. Modification of the rules on the use of cookies.

Small files of alphanumeric data, known as "cookies", may be stored onto a user's device during a browsing session enabling a website provider to recognise that device during a user's subsequent access of the site. Whilst this can improve the speed and functionality of a user's website experience it may allow providers and third parties (such as advertisers) to obtain personal information often without the user's knowledge.

Under the previous regulations a provider was obliged to inform people how it used the cookies stored and had to give them an option to opt-out if they objected. The amended Regulations hand more control to the user in that a provider may now only place a cookie on a machine with the user's consent. The system is changing from one of "informed opt-out" to one of "prior, informed opt-in". Whilst the Information Commissioner's Office (the "ICO") does not prescribe how the implementation is to take place, it does give examples of possible approaches in its guidance notes recently published[3].

1 The Privacy and Electronic Communications (EC Directive) Regulations 2003 (SI 2003/2426) as amended by The Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2011 (SI 2011/1208).
2 2002/58/EC Directive on privacy and electronic communications.

3 http://www.ico.gov.uk/~/media/documents/library/Privacy_and_electronic/Practical_application/advice_on_the_new_cookies_regulations.pdf

2. New restrictions on sending "spam".

The amended Regulations further restrict the sending of unsolicited electronic mail for direct marketing purposes. Direct marketers must now be clearly identified where commercial communications are made on their behalf. Any such communications should also inform of any related promotional offers, competitions or games and qualifying conditions. The new restrictions on spam stop short of the revised E-Privacy Directive's provisions, which provide for those with an interest in combating unsolicited commercial e-mails to take action in civil proceedings.

3. New requirements on ISPs and telecommunications service providers to ensure data security.

Providers of public electronic communications services must implement security policies on processing personal data. The ICO has the power to audit such policies. Where a service provider fails to notify a personal data breach the ICO may issue a fine of £1,000. Unless a service provider can satisfy the ICO that it is unnecessary to do so, it must also advise subscribers or users of such breaches if they are likely to be adversely affected.

4. Access to personal data by the police and security services.

The amended Regulations permit the police and security services to request access to personal data and to compel service providers to establish and maintain procedures for responding to such requests. There is no reference to what conditions must first be satisfied to enable the authorities to obtain such data.

5. Increased investigatory and enforcement powers available to the ICO.

The ICO may impose a penalty of up to £500,000 for serious breaches of the amended Regulations and the significant increase in available fines is in line with the recent increase for data protection violation under the DPA[4]. However the government has stopped short of including the use of criminal sanctions, which the revised E-Privacy Directive provides for "where appropriate".

Commentary

The ICO has now published guidelines[5] on enforcement of the new laws which indicate that with respect to the new rules on cookies businesses and organisations will have up to one year to "get their house in order" before ICO enforcement begins, although this does not mean they can simply sit back and do nothing towards achieving compliance in the meantime. It is helpful that the ICO's own website already publishes a revised statement for users on the use of cookies, taking into account the new laws. This clearly features the user "opt-in" and businesses could perhaps use it as a model of one way to implement the required change.

Civil liberties campaigners are likely to be disturbed by the new powers of the police and security services to request access to personal data. Although the ICO guidelines referred to above indicate that the ICO will allow a lead-in time of three months before considering enforcement, they do not clarify the circumstances in which these powers may be deployed.

HFW Tip

Those responsible for the provision of company websites, whether from a legal, technical or managerial perspective, should ensure a timely review of their policies and conditions of use on the handling of personal data to ensure compliance with the new laws.

For more information, please contact Anthony Woolich, Partner, on +44 (0)20 7264 8033 or anthony.woolich@hfw.com, or Martin Hill, Associate, on +44 (0)20 7264 8427 or martin.hill@hfw.com, or Philip Thomas, Associate, on +44 (0)20 7264 8400 or philip.thomas@hfw.com or your usual HFW contact.

4 Data Protection Act 1998 (as amended).
5 http://www.ico.gov.uk/~/media/documents/library/Privacy_and_electronic/Practical_application/enforcing_the_revised_privacy_and_electronic_communication_regulations_v1.ashx

HOLMAN FENWICK WILLAN LLP
Friary Court, 65 Crutched Friars
London EC3N 2AE
T: +44 (0)20 7264 8000
F: +44 (0)20 7264 8888