

Q. What is the revised ePrivacy Directive?

A. The revised ePrivacy Directive is part of a broader piece of European legislation (the EU Electronic Communications Framework) comprising a total of five Directives which was required to be implemented into all national laws by 25 May 2011. As at April 2012, 19 out of 27 EU countries have actually done so. In the UK the Directive is transposed into national law as the Privacy & Electronic Communications (EC Directive) (Amendment) Regulations 2011.

Q. Why is it important for advertising and the internet?

A. The revised EU ePrivacy Directive covers the use of internet “cookies” and other technologies that – among other things – facilitate online advertising. Article 5.3 of the revised Directive replaces the existing “notice and opt out” provisions for the use of such technologies with a requirement to obtain consent for *“the storing of information or the gaining of access to information stored in the terminal equipment of a subscriber or user... having been provided with clear and comprehensive information”*. It therefore, applies to all technologies used for this purpose - including cookies. There is an exemption when uses are *“strictly necessary”* for the service explicitly requested by the user (eg shopping baskets).

Q. What does this mean in practice?

A. While the Directive requires only “consent”, if it is implemented too strictly it could introduce an ‘opt in’ regime for many cookie uses. This could be very disruptive for the consumer requiring them to tick a box or pop-up when every cookie is dropped. Equally it would be detrimental to the advertising business models that underpin content and services on the internet. For an example of how repeated ‘opt in’ prompts affect web browsing see: www.cookie demosite.eu.

Q. What’s the view of the UK Government?

A. The UK Government recognises the revised Directive is a *“well-meaning regulation that will be very difficult to work in practice”*. It takes a pragmatic view which is confirmed in an ‘open letter’ clarifying its approach. The letter was drafted in full consultation with the Information Commissioner’s Office (ICO) – the UK’s data protection authority that will enforce the UK law. This ‘open letter’ is at www.dcms.gov.uk/images/publications/cookies_open_letter.pdf.

In a nutshell, the UK Government supports an approach based upon an ‘ecology of [industry] solutions’. So there is no ‘one size fits all’ and the UK Government explicitly supports the advertising industry’s EU self-regulatory initiative which introduces a small symbol or icon in website ads and seeks to enhance transparency and consumer control for tailored advertising based upon previous web browsing activity. For further details see www.youronlinechoices.eu/goodpractice.html.

Q. The ICO will enforce the new law – does it agree with the UK Government?

- A. The ICO also believes in a balanced approach and this is enshrined in the various versions of guidance it has published (see below).

It has provided organisations with a year’s ‘lead in’ (from when the UK law was enacted in May 2011) to work towards compliance. The latest version of its guidance is available at: www.ico.gov.uk/news/blog/2012/updated-ico-advice-guidance-e-privacy-directive-eu-cookie-law.aspx. The guidance provides greater clarity on ‘implied consent’, specifically that it is a valid form of consent and can be used to comply with the new law, as long as you know that internet users understand what’s going on.

Q. So what should businesses be doing to comply?

- A. Businesses should review the good practice that is already live. In addition to this, the IAB has published a simple and practical five step guide on what businesses should be doing to work towards compliance (see below). The IAB will be following these steps on its own site.

Five Practical Steps Towards ePrivacy Compliance:

1. **Get to grips with how your site works or what technology you’re working with.** Carry out ongoing audits of your use of cookies and other technologies so that you know what you’re working with or what’s being dropped on your site. Document everything!
2. **Be very clear and transparent on how you present information to consumers.** Revisit your privacy policy and make sure that you are being clear and transparent on the technologies that are being used. It is advisable to take a ‘layered approach’: start simply and offer further and more detailed information for those consumers that want to find out more. You can point to helpful websites such as www.aboutcookies.org or – if appropriate - www.youronlinechoices.eu.
3. **Deliver prominence.** Make your privacy information more prominent on your site. Place it ‘above the fold’ and use a different font or colour. You can also label it something a little more eye catching. Instead of ‘privacy policy’ why not ‘how does this website work?’ or ‘how do we collect and use your information?’
4. **Context is king!** Consider ways to achieve informed consent in a contextual way. This will depend on what activity you are seeking to derive consent for but a good way to do this is via a simple and discrete one-time ‘banner overlay’ or pop up using clear and simple language and linking to ways for people to control cookies or other technologies.
5. **Join the EU advertising self-regulation programme.** If you are a third party active in behavioural advertising (including retargeting) then you should be involved in the EU self-regulatory initiative. As part of this businesses are rolling out an icon in ads linked to clear and transparent information and mechanisms of control. Publishers can also host the icon on their web pages. If you’re an agency or advertiser then you should make sure that your data partners are involved. If you want to know more (and to also see who is involved) go to: www.youronlinechoices.eu/goodpractice.html.

For full details see: www.iabuk.net/blog/tackling-the-eprivacy-conundrum.

For further information contact Nick Stringer, IAB director of regulatory affairs at nick@iabuk.net.

IAB UK, May 2012