

# Client Alert

Latham & Watkins  
Corporate Department

## UK Cookie Rules: Are you Compliant?

*The UK Information Commissioners' Office (ICO) 12 month grace period for enforcing compliance with the [new cookie consent rules](#) has now expired. If you are not yet compliant, you need to take action.*

Over the course of the 12 month grace period, we have seen guidance released from, amongst others, the ICO, setting out its interpretation of the new rules; the International Chamber of Commerce (ICC), working with industry to publish a helpful guide for website operators; and the Internet Advertising Bureau (IAB), proposing a self-regulatory compliance scheme for online advertisers.

The ICO's consolidated guidance promotes a transparent and proportionate approach, and makes clear that it expects organisations to understand exactly what cookies and other technology that collect user information (collectively referred to as cookies in this *Alert*) are used on their site (by both the organisation itself and third party advertising networks), to take steps to give clear and accessible information to users and to obtain appropriate consent for such cookies. The ICO also makes clear that implied consent can be a valid option, depending upon the quality and accessibility of the information provided to the user. Implied consent does not however equate to doing nothing with your site and presuming that the user understands what you use cookies for and consents merely by using the site.

In terms of cookies set to track browsing for the purposes of targeted advertising (seen as the most intrusive use of cookies), the ICO emphasises that website operators and third party advertising networks must work together to ensure the required consent is obtained. Responsibility ultimately lies with the person setting the cookie (*i.e.* the third party ad network), but in practice, the operator of the consumer facing site is best placed to obtain such consent, with the assistance of the third party to understand exactly what cookies are being used and how. The Article 29 Working Party (a body comprised of representative of each EU privacy regulator) has made clear in its recent [Opinion 4/2012](#) on the cookie rules exemptions that consent will always be required for third party advertising cookies, with no applicable exemptions (confirming its long standing view — see [Opinion 2/2010](#) and [Opinion 16/2011](#) — that targeting advertising cookies are intrusive and require the highest standard of consent).

### The ICC Approach

The ICC guide was developed to help website operators standardise terminology, by dividing cookies into four categories and providing standard disclosures for each, in the hope that consistency will expedite increased consumer understanding.

"Implied consent can be a valid approach, but this does not equate to doing nothing with your site and presuming that the user understands what you use cookies for and consents merely by continuing to use it."

The four cookie categories are as follows:

1. Strictly necessary (essential in order to use the site and receive services, e.g. online shopping basket functionality, session cookies for managing security tokens throughout the site, multimedia flash cookies enabling media play back, load balancing session cookies, user interface customization session cookies etc.);
2. Performance (aggregate / anonymous tracking of how users use the site, e.g. analytics cookies, error management cookies);
3. Functionality (to enable certain site functionality, e.g. to provide localised information, auto-completing usernames, remembering customised settings over multiple browser sessions or previous suppressions of services by the user etc.);
4. Targeting / advertising (to target advertising to user relevance, to track advertising click-throughs, etc.)

The guidance has been well received by the ICO, but has not been commented on by the Article 29 Working Party – it is nonetheless a great starting point when analysing your cookie use and when putting in place cookies notices and disclosure statements.

## **The IAB Guidance**

The IAB has also issued guidance for its members (e.g. those in the targeted advertising industry), setting out a self-regulatory scheme based around an icon to be displayed by all targeted adverts and links to further information, so that the user understands that targeted advertising is in place and the advertising network is using cookies on the users PC. If clicked, the icon takes users to the [youronlinechoices.eu](http://youronlinechoices.eu) site which explains how targeting advertising works and allows the user to opt-out of targeted advertising (but not advertising in general) from all or any one or more of the advertisers in the IAB's network. The Article 29 Working Party, whilst welcoming the initiative, stated that it alone was insufficient to obtain valid consent to the setting of cookies for targeted advertising (or for associated cookies, such as frequency capping, ad affiliation, de-bugging or click fraud prevention cookies), as the icon is not currently meaningful to consumers; insufficient information is provided to the user about the relevant cookies; and the scheme provides for consent on a generic, opt-out basis which does constitute valid consent in this context, where anything short of informed, active consent will be inadequate.

## **Compliance Approaches In Practice**

In practice, we are seeing a range of compliance approaches being taken by businesses operating in the UK, ranging from banner notices with tick boxes for active consent (the only example of which we have seen is the ICO's solution), to one-time banners or pop-overs (such as those adopted by the *BBC* or *Financial Times*) giving brief information and allowing the user to take steps to disable the site's cookies if they wish to do so before continuing to use the site ("implied" consent). There are very few examples of express "opt-in" consents, and most website operators seem to be taking an implied consent approach, with some offering users an "opt-out" mechanism, and others relying on users blocking cookies through browser settings (or simply ceasing to use the website).

Methods of informing users of cookie usage in order to ensure any implied consent is "informed" vary in their intrusiveness and persistence. For example, *The Telegraph's* popover appears at the bottom of the window and disappears once the user navigates to another page on the site. By contrast, the *Financial Times'* popover must be dismissed by the user before browsing is permitted. Similarly, whilst some banner notices appear only on the home page and disappear once the user navigates to a different page (e.g. *BBC*), others (such as *Channel 4's*) persist across the whole site until dismissed by the user. Whilst the more persistent and intrusive

solutions are more likely to result in obtaining informed consent if challenged, they are also more disruptive to the user experience.

As noted above, website operators have also taken different approaches in implementing opt-out functionality enabling users to modify their cookie settings. Some website operators (e.g. BBC and BT) offer the user a control panel where all but strictly necessary (ICC category 1) cookies can be disabled. Other operators, however (e.g. Channel 4), simply explain how users may disable cookies in their web browser settings.

Some website operators have implemented separate cookies policies alongside full privacy policies to give users information about the types of cookies in operation on their website. We are also seeing a significant number adopt the ICC categories as a way of explaining the various purposes of the different cookies.

You can access our detailed review [here](#).

## Your Next Steps

If you are not yet compliant, then you should take the following steps as soon as possible:

- Conduct a full audit of the cookies on all websites operated by your organisation to determine which categories of cookie each site uses and for what purposes, so you have the information needed to develop a proportionate compliance approach.
- Produce a cookies policy (or review the wording of your existing cookies or privacy policy) to explain which cookies you use, and why you use them. Consider using the ICC categories to guide your users.
- At the very least, explain in your cookies policy how customers can disable non-essential cookies through browser settings, and consider implementing a control panel on the site itself to allow cookies to be disabled in a more granular manner. Such an approach has the advantage of allowing users to disable some but not all of your site's cookies.
- Consider how to obtain consent from users if required e.g. whether to rely on implied consent or express consent; whether to use an opt-in consent (in which case your site should not set any cookies prior to receipt of such consent) or an opt-out approach (where the user is merely informed that the site sets cookies and told how to disable them).
- Consider the wording of your consent notice carefully to be certain that it allows the user to provide informed consent, whilst minimising the risk that the user will elect to disable cookies *i.e.* try and strike the elusive balance between describing what your cookies do in plain English without scaring consumers into de-activating them.
- Consider how to display the consent request / notice on your website, e.g. through a popover or banner-type interface, and whether the user must respond to the notice prior to interacting with other site content.

Latham & Watkins can provide advice and guidance to assist you in developing a workable compliance solution, including advising on:

- The relative merits of opt-in vs. opt-out consent and various notice methods in relation to the specific cookies you use on your website.
- Drafting and updating your cookies and privacy policies.
- Providing optimal consent wording to mitigate risk of non-compliance.
- General privacy and data protection law advice concerning your web presence.

If you have any questions about this *Client Alert*, please contact one of the authors listed below or the Latham attorney with whom you normally consult:

**Gail E. Crawford**  
+44.20.7710.3001  
gail.crawford@lw.com  
London

**Amy Taylor**  
+44.20.7710.4785  
amy.taylor@lw.com  
London

**Ben Wright\***  
+44.20.7710.4673  
ben.wright@lw.com  
London

\* Ben Wright, a solicitor trainee in Latham & Watkins London office assisted in the preparation of this Alert.

---

*Client Alert* is published by Latham & Watkins as a news reporting service to clients and other friends. The information contained in this publication should not be construed as legal advice. Should further analysis or explanation of the subject matter be required, please contact the attorney with whom you normally consult. A complete list of our *Client Alerts* can be found on our website at [www.lw.com](http://www.lw.com).

If you wish to update your contact details or customise the information you receive from Latham & Watkins, visit <http://events.lw.com/reaction/subscriptionpage.html> to subscribe to our global client mailings program.

<b>Abu Dhabi</b>	<b>Houston</b>	<b>Paris</b>
<b>Barcelona</b>	<b>London</b>	<b>Riyadh*</b>
<b>Beijing</b>	<b>Los Angeles</b>	<b>Rome</b>
<b>Boston</b>	<b>Madrid</b>	<b>San Diego</b>
<b>Brussels</b>	<b>Milan</b>	<b>San Francisco</b>
<b>Chicago</b>	<b>Moscow</b>	<b>Shanghai</b>
<b>Doha</b>	<b>Munich</b>	<b>Silicon Valley</b>
<b>Dubai</b>	<b>New Jersey</b>	<b>Singapore</b>
<b>Frankfurt</b>	<b>New York</b>	<b>Tokyo</b>
<b>Hamburg</b>	<b>Orange County</b>	<b>Washington, D.C.</b>
<b>Hong Kong</b>		

\* In association with the Law Office of Mohammed A. Al-Sheikh