



Business concern over new EU consent requirement to use website cookies

New EU cookie consent requirement

Amendments to the EU's ePrivacy Directive have meant that since 25 May 2011 the EU has required website operators to obtain the consent of users to the use of cookies. This is a significant development and it is causing considerable concern among businesses. The new consent requirements for use of cookies, which consist of small text files that are used by virtually every website to recognise a user's computer and collect information on a user's activities and preferences, has caused a storm of debate as regulators and businesses struggle to find a practical way of obtaining consent.

There is also particular concern regarding compliance with the new requirements in relation to so called "third party" or "tracking" cookies used in behavioural advertising, where information from cookies is shared with third parties. In these circumstances obtaining consent may be more complex and care needs to be taken to make sure users are made aware of what data are being collected and by whom.

There is only one exception to the new EU consent requirement where the website is using a cookie "that is strictly necessary" to provide the service explicitly requested by the user. However, this is a narrow exception covering, for example, use of a cookie to allow the website to remember items placed in a virtual shopping basket and would not apply, to use of cookies to collect website analytics data.

Confused transposition process in the EU

Another particular concern is the lack of a harmonised approach to implementation of the new consent requirements in different EU Member States. Despite the 25 May 2011 implementation deadline only ten EU Member States have yet implemented the requirements into their national laws, including Estonia, Finland, Ireland, Latvia, Lithuania, Malta, Sweden, Hungary, Luxembourg and the UK. The table on page 3 summarises the current position.

There is also a lack of clarity on how in practice consent may be obtained and in particular whether browser settings can be used to obtain consent. It is understood that in Ireland, Luxembourg, Sweden and the UK the implementing legislation or guidance expressly provides that consent may result from the browser settings. Of these early adopting

This **Sidley update** has been prepared by Sidley Austin LLP for informational purposes only and does not constitute legal advice. This information is not intended to create, and receipt of it does not constitute, a lawyer-client relationship. Some of the information in this update is based on views of local counsel which is likely to change and where Sidley Austin LLP is not admitted. Readers should not act upon this without seeking advice from professional advisers.

Attorney Advertising - For purposes of compliance with New York State Bar rules, our headquarters are Sidley Austin LLP, 787 Seventh Avenue, New York, NY 10019, 212.839.5300 and One South Dearborn, Chicago, IL 60603, 312.853.7000.

Prior results do not guarantee a similar outcome.

Member States national guidance has only been published, so far, in Ireland, Sweden and the UK although further national guidance may be published in due course.

In the UK, the Information Commissioner's Office (the "ICO") has issued guidance on what may constitute a sufficient opt-in consent:

- **Pop ups and similar techniques** – using pop ups on the website screen for users to click that they consent to use of cookies, although the ICO acknowledges that this could spoil the user experience.
- **Terms and conditions** – when users open an online account, or sign in to use the services, they could consent through terms and conditions to operation of the account and to use of cookies but a positive indication of consent is required such as through the user ticking a box.
- **Settings-led consent** – obtaining consent as part of the process by which the user confirms what they want to do, or how they want the site to work, for example, when selecting a feature as to the size of text they want displayed.
- **Feature-led consent** – placing text in the footer or header of the web page which is highlighted or which turns into a scrolling piece of text when wanting to set a cookie on the user's device.
- **Browser settings** – using browser settings to obtain consent, although the view of the ICO is that most browser settings are not sophisticated enough to allow a website provider to assume that the user has given their consent to the website using a cookie.

To allow businesses to achieve compliance the UK has a grace period of 12 months until May 2012 during which time the ICO will refrain from using its enforcement powers although businesses are expected to take steps to comply with the new requirements. It is also understood that in Sweden a grace period, expected to be around 6 months, will also be applied.

Another question that is still not clear is whether national Member State laws implementing the new cookie consent requirement will apply to website operators not established in a Member State, for example a US website accessed by French consumers.

Practical steps to be considered by businesses now

While there are still some unanswered questions concerning the implementation and scope of the new EU cookie consent requirement it is important that website operators start to consider the new requirements now and how they may apply to their business. Some practical steps that can be taken now include:

- monitoring the implementation of the cookie consent requirement in different Member States over the next few months;
- carrying out an audit of the business use of cookies, including the type of cookies used (e.g. first party or third party cookies, session only cookies or persistent cookies);
- updating privacy policies to include more explicit disclosures on the use and ability to opt-out of use of cookies;
- evaluating consent options, taking into account customer impact, costs and applicable laws; and
- reviewing existing arrangements with service providers concerning the collection of data and use of cookies.

Table: Summary of EU Implementation as at 1 August 2011

EU Member State	Date of national implementation or current status	Can I use a browser to obtain consent? ¹	National guidance currently available?
Austria	Draft Bill		
Belgium	Draft Bill	Yes	
Bulgaria	Draft Bill		
Cyprus	Draft Bill		
Czech Rep.	Draft Bill		
Denmark	Draft Executive Order		
Estonia	25 May 2011		
Finland	25 May 2011		
France	End of Sept 2011	Yes	
Germany	Draft Bill	Yes	
Greece	Draft Bill		
Hungary	20 July 2011		
Ireland	1 July 2011	Yes	Yes
Italy	Draft Bill		
Latvia	8 June 2011		
Lithuania	1 Aug 2011		
Luxembourg	13 Aug 2011	Yes	
Malta	24 June 2011		
Netherlands	Expected Jan 2012		
Poland	Public Consultation	Yes	
Portugal	Draft Bill		
Romania	Draft Bill		
Slovakia	Effective 1 Oct 2011	Yes	
Slovenia	Draft Bill	Yes	
Spain	Draft Bill	Yes	
Sweden	1 July 2011 (grace period)	Yes	Yes
UK	26 May 2011 (12 month grace period)	Yes	Yes

¹ Based on adopted or draft legislation or based on views of Government authorities or national Data Protection Authorities. Some of the information in this update is based on views of local counsel which is likely to change and where Sidley Austin LLP is not admitted.

For further details on the current implementation of the EU cookie consent requirements please contact:

John Casanova, Partner

jcasanova@sidley.com

+44 (0)20 7360 3739

Jens Rinze, Partner

jrinze@sidley.com

+49 69 22 22 1 4020

William Long, Counsel

wlong@sidley.com

+44 (0)20 7360 2061

The Privacy, Data Security & Information Law Practice of Sidley Austin LLP

We offer clients an inter-disciplinary, international group of lawyers focusing on the complex national and international issues of data protection and cyber law. The group includes regulatory compliance lawyers, litigators, financial institution practitioners, healthcare lawyers, EU specialists, IT licensing and marketing counsel, intellectual property, and white collar lawyers. Sidley provides services in the following areas:

- Privacy and Internet Litigation and Regulatory Advice
- Data Breach, Incident Response, and Cybercrime Advice
- Global Data Protection and Information Security
- International Data Transfer Solutions
- Outsourcing and Cross-Border Issues
- Gramm-Leach-Bliley and Financial Privacy
- HIPAA and Healthcare Privacy
- Workplace Privacy and Employee Monitoring
- Cyberlaw, E-Commerce, and Internet Issues
- Unfair Competition and Consumer Protection
- Trademark and Copyright Litigation and Counseling
- Website Policies and Domain Name Protection
- Records Retention and Electronic Discovery

To receive future copies of this and other Sidley updates via email, please sign up at www.sidley.com/subscribe

BEIJING BRUSSELS CHICAGO DALLAS FRANKFURT GENEVA HONG KONG LONDON LOS ANGELES NEW YORK
PALO ALTO SAN FRANCISCO SHANGHAI SINGAPORE SYDNEY TOKYO WASHINGTON, D.C.

www.sidley.com

Sidley Austin LLP, a Delaware limited liability partnership which operates at the firm's offices other than Chicago, London, Hong Kong, Singapore and Sydney, is affiliated with other partnerships, including Sidley Austin LLP, an Illinois limited liability partnership (Chicago); Sidley Austin LLP, a separate Delaware limited liability partnership (London); Sidley Austin LLP, a separate Delaware limited liability partnership (Singapore); Sidley Austin, a New York general partnership (Hong Kong); Sidley Austin, a Delaware general partnership of registered foreign lawyers restricted to practicing foreign law (Sydney); and Sidley Austin Nishikawa Foreign Law Joint Enterprise (Tokyo). The affiliated partnerships are referred to herein collectively as Sidley Austin, Sidley or the firm.

SIDLEY AUSTIN LLP
SIDLEY