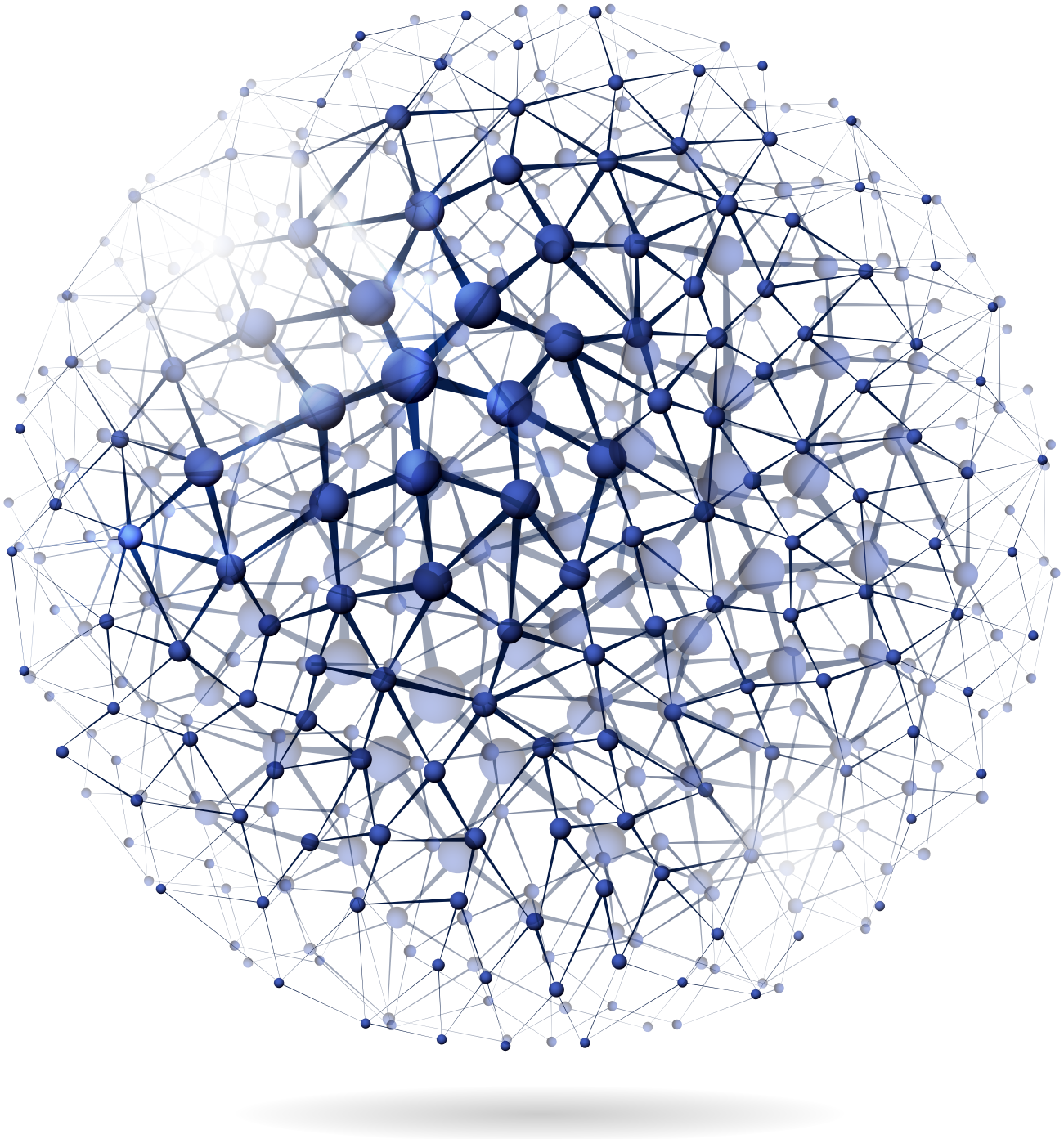
ALLEN & OVERY



Cookie Consent Update 2014

November 2014

How time flies…

It seems only yesterday that everyone was talking about "cookies". While other issues have taken precedence in the minds of many, it is worth reflecting on where we are with the regime for obtaining consent for the use of cookies on websites.

It all began in November 2009 when the European Commission revised an array of telecommunication directives, including the ePrivacy Directive (2002/58/EC) (the Original Directive). Member States had until 25 May 2011 to implement the changes contained in the revised ePrivacy Directive (2009/136/EC) (the Revised Directive) into their local law. One of the provisions that was amended concerned the use of cookies for online behavioural advertising. The Revised Directive changed the previous "right to refuse" regime to a system under which consent must be obtained in order to use cookies for this purpose (with limited exceptions).

Since this happened, EU Member States have been gradually implementing the Revised Directive. There was much debate about what the consent requirements in the Revised Directive actually mean in practice. Some Member States were slow to implement and there have been concerns about a lack of consistency in approach. After the Article 29 Working Party made their opinions on the requirements of the Revised Directive clear, stakeholders feared that they might have to fundamentally change their practices on how cookies are used and how users consent to their use. Others offered less strict views on interpretation.

This publication provides a brief summary of the issues and the views of interested parties. It also looks at how some Member States have interpreted the rules when implementing them.

Use of cookies for advertising

A cookie is a small text or data file which a website implants on the hard discs of visitors to the site. It collects information about users by tracking their browsing habits, acting as a memory of what has happened previously.

There are different types of cookie. Some are less invasive, such as *"session cookies"* which expire at the end of the user's browser session, and help, for example, by remembering items you have placed in your on-line shopping basket. Others, *"persistent cookies"*, remain on the computer and may track what the user is doing across several websites to build up a profile (eg for targeted advertising).

"First party cookies" are planted by the website the user visits. *"Third party cookies"* are placed by third parties.

For example, internet publishers may provide space on their websites to advertising network providers (ANPs) to generate income from those websites. Advertisers place advertisements through the ANPs. To tailor these to a user's needs, ANPs place the third party cookies onto a user's computer to build up a detailed user profile.

There are legitimate business uses for tracking in this manner. However, users will often be unaware it is happening. Even if they are aware, many people do not understand how to refuse, or remove, cookies through their browser settings. This raises privacy concerns as the storage and use of personal data will invariably be involved. It is recognised that these conflicting interests need to be carefully balanced.

The changes to the ePrivacy Directive

The Original Directive permitted the storing of information, or the gaining of access to information already stored in the user's computer, if the user:

– is provided with clear and comprehensive information about the purposes of the processing; and

– is offered the right to refuse such processing.

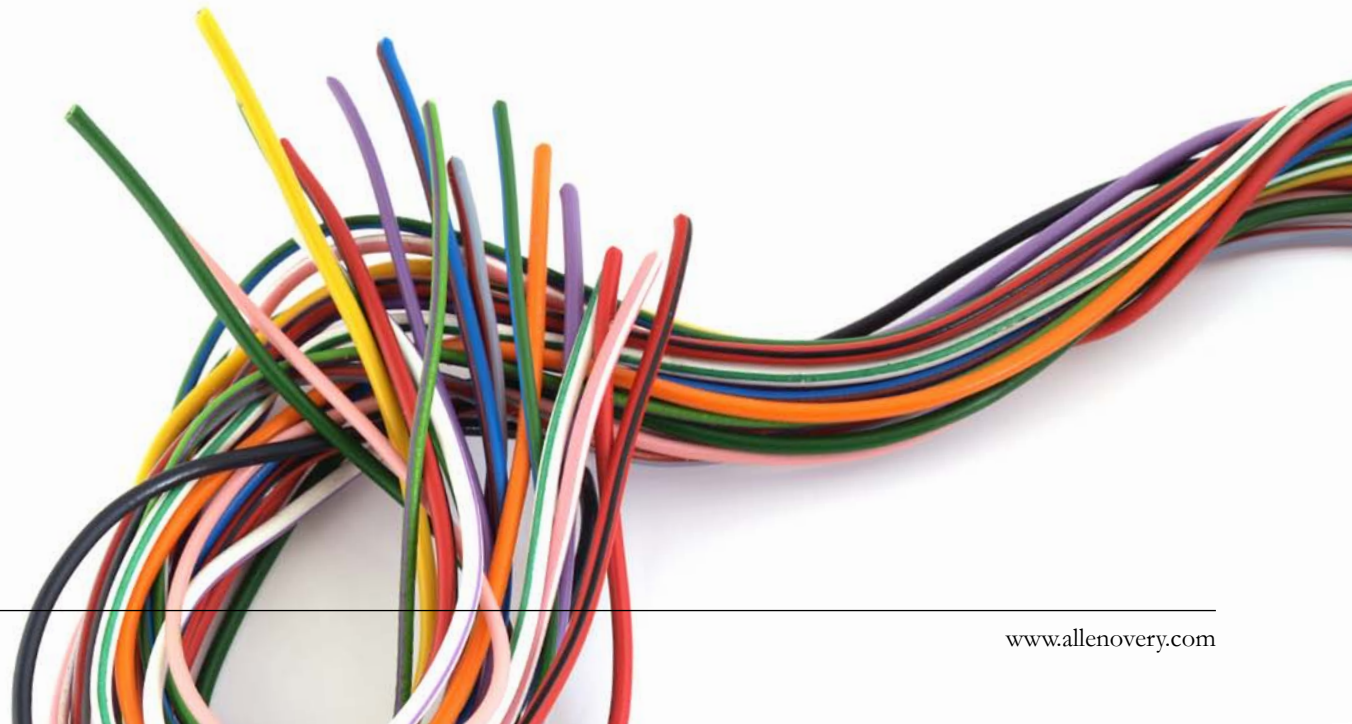
Under the Revised Directive, however, the user must have given his or her **consent** to such processing, having been provided with clear and comprehensive information about the purposes of the processing. This consent must be unambiguous.

Certain cookies are exempt. The consent obligations do not apply to use of cookies which is "strictly necessary" for the provision of services requested by the user (such as secure access to a website) or to use of cookies that are planted for the "sole purpose" of carrying out an online communication. However, these exceptions are interpreted restrictively.

What needs to be done to comply?

For a website operator there are a number of ways in which compliance with the consent requirement can be achieved. A good example is a pop up box that appears when you enter the website. This might give the appropriate information, perhaps links to further information on a separate page explaining the cookies being placed, and asks you to accept the use of cookies on the site before continuing. We will consider below various views on other mechanisms and whether they are thought to be sufficient.

However, the way in which third party cookies are placed makes it much harder to gain valid consent. This is predominantly because there is usually no direct relationship with the user. The ANP would have to either contractually oblige the website operator to obtain the consent on their behalf (which is generally resisted), or create their own consent mechanisms, for example using splash screens or pop up boxes (perhaps in collaboration with other third parties).



What is the view of the Article 29 Working Party?

The Article 29 Working Party (the Working Party) is an independent advisory group composed of representatives of the EU data protection regulators. One of its roles is to make recommendations to try to achieve uniform application of data protection laws across the EU. While its opinions are not currently binding on Member States, they do carry considerable weight.

The Working Party has issued a number of Opinions on this topic. Over the years their views have not changed. We consider below some of their key messages.

Application of the Revised Directive

What should consent look like?

In 2010, the Working Party released a detailed Opinion explaining the issues and concluded that the Revised Directive requires the prior informed consent of the user for use of cookies. It favours a prior opt-in mechanism. For example, with tracking cookies, ANPs should first provide the user with sufficient information on the purpose of the tracking cookie, and they may then place and read the cookies only if the user consents. "Consent" requires a user's affirmative action to indicate they are willing to receive cookies for the specified purposes before the cookie is sent to the user. The consent must be freely given, specific and revocable. This is consistent with the Working Party's Opinion on "consent" published in 2011.

A further Working Party document, published in 2013, sought to clarify previous guidance. The Working Party recognised that practical implementations of the legal requirements vary among website operators across EU Member States. It lists some of the most commonly used practices such as having an immediately visible notice that various types of cookies are being used (linked to further information), informing the user that by using the website they agree to cookies being set, explaining how to signify and later withdraw consent; and providing a mechanism whereby a user can accept or decline some or all cookies. It points out that, used alone, these mechanisms will probably not amount to valid consent – they will need to be used in combination.

A consent mechanism should include each of the following four main elements:

- specific information – a clear visible notice on the use of cookies (with access to necessary information);
- prior consent – before the data processing starts;
- indication of wishes expressed by user's active behaviour, eg clicking a button (not just following a link); and
- an ability to make a real and meaningful choice with an opportunity to change your mind later.

How should information be provided?

A Recital to the Revised Directive mentions that the methods of providing information, and offering the right to refuse, should be as user-friendly as possible. Therefore, the Working Party recommends that a minimum of information should be provided directly on the screen, and be interactive, easily visible and understandable. Information must not be hidden within a privacy statement or within general terms and conditions.

The Working Party notes that creativity is welcome when it comes to the provision of information and acknowledges that there may be many ways to do this. It specifies that icons placed around advertising on the publisher's website with links to additional information is an example they find "both positive and necessary".

Finally, the Working Party considers that it is essential for ANPs to inform users "periodically" that monitoring is taking place.

Does the Working Party consider browser settings sufficient?

Recital 66 to the Revised Directive states that the user's consent can be expressed by using the relevant settings of a browser where it is technically possible and effective. However, the Working Party believes that this will form valid consent in very limited circumstances. It is generally agreed that current browser settings are not sophisticated enough to ensure compliance. Browser manufacturers and regulatory bodies in the EU and the US are working on changing this.

If the browser used is set to accept cookies by default, the Working Party feels that the user cannot be deemed to have consented. Average users are not aware of their online behaviour being tracked, and so their inaction could not indicate their wishes. Browser settings could, according to the Working Party, give valid consent if a browser by default rejects cookies and the user actively has to change the settings to accept cookies.

What about cookie-based opt-out mechanisms?

Cookie-based opt-out mechanisms allow users to indicate their desire to opt-out of being tracked, via the ANP's website. The Working Party generally finds this practice to be insufficient to deliver prior informed consent, as users commonly do not realise that processing is taking place, or don't know how to exercise the opt out, and therefore would not be giving informed consent by simply not opting out.

Can the exemptions be relied upon?

A Working Party Opinion adopted in 2012 on "Cookie Consent Exemption" considers the exemptions (eg cookies which are "strictly necessary") in detail. It makes it clear that third-party cookies used to track user behaviour to enable the serving of targeted or online behavioral advertising are not covered by either of these exemptions. As a general rule, the exemptions are narrowly defined.

Would you need consent every time a cookie is placed?

The Working Party is of the opinion that single acceptance to receive a cookie could provide consent to subsequent monitoring of a user's internet browsing. However they suggest that ANPs should:

– limit in time the scope of the consent;

– offer the option to easily revoke consent; and

– create a visible interface tool, to be displayed whenever monitoring takes place.

Is the data collected by tracking cookies always personal data?

We are reminded by the Working Party that storing information by way of cookies can involve processing of personal data (particularly with tracking cookies), and data protection legislation will therefore also apply. In a UK case earlier this year (*Vidal Hall & Ors v Google Inc*), the Judge went even further and having found that misuse of private information is a tort, held that behavioural information deserves the same protection as fully identifiable data, even if it is in a pseudonymised state, eg where a cookie has a unique user ID.

Can access be conditional on accepting the cookies?

Access to content on a website may only be conditional on well-informed acceptance of cookies if this is for a legitimate purpose. It should only apply to certain content on the site (not the site generally), according to the Working Party in their 2013 Working Document. The Working Party does recognise that in some Member States, such as in Sweden, websites are allowed to require that consent is given to cookies in order to gain access to the website.

What other views have been expressed?

While the Working Party has taken a fairly strict view of the consent requirements, others have taken a slightly different view.

Neelie Kroes (Vice-President of the European Commission responsible for the Digital Agenda) initially took a more pragmatic view. She stressed the need for "a user friendly solution" but "possibly based on browser (or another application) settings". On that basis, she thought that it would be "prudent to avoid options such as recurring pop-up windows. On the other hand it would not be sufficient to bury the necessary information deep in a website's privacy policies". However, in 2012 she stated that a proposed 'do not track' system (which refuses cookies) that was being developed by a working group of the Worldwide Web Consortium was not sufficient to comply with the Revised Directive.

MEP Nuno Alvaro, the rapporteur for the Revised Directive stated that consent did not need to be "prior and/or explicit". When the issue was discussed in formulating the text of the Revised Directive, this language was rejected in favour of a more flexible approach. He pointed out that Recital 66 makes it clear that browser settings could be considered an indication

The European Advertising Standards Alliance (EASA) and the Interactive Advertising Bureau Europe (IAB) adopted, in April 2012, what was referred to by the Working Party as the EASA/IAB Code. The EASA/IAB Code advocates the use of a uniform pictogram or icon alerting a user receiving targeted advertising. A hyperlink is found with the icon which will link to a website providing consumer guidance on online behavioural advertising. However this was not well received by the Working Party which highlighted several shortcomings of the EASA/IAB Code, including that it failed to provide internet users with the necessary information about the use of tracking cookies; that it only allowed users to exercise choice on an opt-out basis; and that it did not make it clear that an opt-out might only relate to the serving of targeted advertising rather than the tracking of user behaviour itself. It is worth noting that the IAB never intended the EASA/IAB Code to achieve compliance but rather to create a level playing field. They state that the EASA/IAB Code is "in addition" to applicable law.

What have Member States done?

Given the differing views in relation to the requirement for consent, it is hardly surprising that Member States have approached implementation of the Revised Directive in different ways. Their priorities clearly lie in balancing their own economic interests with the privacy rights of individuals. However, arguably, the approaches taken are gradually converging, perhaps assisted by the consistent message coming from the Working Party.

BELGIUM

In Belgium, the use of cookies is regulated by article 129 of the Belgian Electronic Communications Act 2005 (ECA). This article implements the Original Directive as amended by the Revised Directive.

According to article 129 of the ECA, the storage and the use of cookies on a subscriber's or user's end equipment is subject to the following conditions: (i) the subscriber or user needs to be provided with clear and comprehensive information about the purposes of the processing and rights in accordance with the Belgian Data Protection Act of 1992, and (ii) after having received this information, the subscriber or user needs to give his consent.

Consent is not required where the cookies are used for technical storage or access with the sole purpose of carrying out transmission of a communication by an electronic communication network, or where strictly necessary to provide an information society service expressly requested by the subscriber or user.

Essentially, the former Belgian "opt-out" regime has been replaced by a "prior, informed opt-in" regime, almost identical to the text of the Revised Directive.

On 24 April 2014, the Belgian Data Protection Authority launched a public consultation on a draft recommendation regarding cookie usage. This contains definitions, sets out things to consider, and provides practical guidance such as listing examples of several categories of cookies and similar technology. The draft recommendation also provides guidance and examples on how to comply with the "prior consent" requirement and provides concrete examples of cookies which it considers to be exempt from this requirement.

The Belgian DPA does not consider browser settings appropriate for obtaining consent. However, in the draft recommendation it does state that "further browsing" can be considered as active behaviour which expresses unambiguous consent if the user has received adequate information and has had the opportunity to express a choice.

The Belgian Data Protection Authority has invited stakeholders to give their input on the text of the draft recommendation by 31 July 2014, following which a final (revised) version of the recommendation will be published.

FRANCE

The Revised Directive was implemented into French law through an Order of 24 August 2011 (n°2011-1012) which amended article 32-II of the French Data Protection Act 1978. In addition, the French Data Protection Authority (the CNIL) issued a set of guidelines which relate to the use of cookies in 2013 (Deliberation n°2013-378) in order to clarify the application of article 32-II.

According to the CNIL, the Revised Directive requires the prior consent of the user for the use of cookies. Such consent should be "free, specific and informed" which entails the delivery of visible, complete, simple and comprehensible information regarding the purpose(s) of the use of cookies and the ability to refuse the use of cookies (generally or for certain specified purposes only) with no substantial negative consequences and the right to access the internet services in the case of refusal. The user's consent should be expressed through a "positive action" which is interpreted in a pragmatic way by the CNIL. Prior consent to the use of cookies is implied in cases where a user continues to browse the website (by clicking on a website's element such as a link or an image, for instance) after having been properly informed of the use of cookies for specified purposes and about the ways in which they can oppose such use.

The CNIL introduced a thirteen-month validity period for prior consent. As a consequence, a cookie remains valid for thirteen months only from its first placement following the expression of consent.

In relation to browser settings, the general view of the CNIL is that current browser settings do not allow a user to manage technologies other than HTTP cookies. Therefore, it is not possible to give consent via browser settings for cookies other than HTTP cookies.

The CNIL provided guidelines on the conditions under which analytical cookies may fall within the exemption from prior consent:

- the user should be provided with required information and have the ability to refuse the use of analytical cookies
- the sole purpose of analytical cookies should be the measurement of audiences on websites through the production of anonymous statistics: collected data should not be combined with other types of data processing operations (eg client data or attendance statistics of other websites) and analytical cookies should not be used to track the user's browsing activity on other applications or websites
- use of an IP address to find a user's location should not determine the position more precisely than the city
- data retention for cookies should not exceed thirteen months.

GERMANY

In Germany, the Federal Council introduced a bill to the German parliament in 2011 that was supposed to implement the Revised Directive into national law. As it was not adopted, opt-in mechanisms are still not required by national German law. However, the Revised Directive might have become directly applicable as the implementation period lapsed on 25 May 2011.

Currently the German Government and the European Commission are in discussions because Germany has reached the conclusion that the current law does not need to be amended and already complies with the Revised Directive. The current law permits the creation of user profiles for the purposes of advertising if (i) a pseudonym (eg a cookie ID) is used, (ii) the user does not object and (iii) the user is informed of his or her right to object. The user profile may not be combined with data on the user. The outcome of the consultations between the European Commission and Germany remains to be seen.

ITALY

The Revised Directive was implemented into Italian law by Legislative Decree no. 69 of 28 May 2012. This amended section 122 of Legislative Decree no. 196 of 30 June 2003 (the Italian Data Protection Code). The Italian DPA also recently passed a specific Resolution "Simplified Arrangements to Provide Information and Obtain Consent Regarding Cookies" on 8 May 2014, which was published in the Italian Official Gazette on 3 June 2014 and covers collecting user consent for use of cookies.

The Resolution clarifies the substantial difference between *"technical cookies, analytics cookies and functional cookies"*, the placement of which does not require prior consent of the user (although they should be informed as the website owner deems appropriate, eg in the privacy policy) and *"profiling cookies"* (used to create a profile of the user, on the basis of their browsing, and send tailored advertising messages) which are subject to the prior, informed consent of the user.

Where profiling cookies are installed, a specific and clearly visible banner must be shown to users when they access the website homepage. The Resolution sets out what the banner should include, such as information that the site is using profiling cookies to send targeted advertising, that they allow the sending of third party cookies (if that is the case), that more detailed information is available through an extended information notice (which must be linked to in the banner), that the user may deny consent to certain or all of the cookies through this extended information notice, and that if the user continues browsing by accessing another section of the site or selecting an item, use of profiling cookies shall be deemed to be approved. Like some other Member States, the Italian DPA therefore considers that acceptance requires an express, even if minimal, action. This could include continuing to browse by selecting any item under the banner as this would demonstrate that the user (i) was aware of the use of the profiling cookies on the website; and (ii) decided in any case to proceed with their browsing activities. Example wording is provided for the banner.

The website manager must keep track of the consents given. They need not display the banner again for subsequent visits to the website by that same user, it being understood that the user should be able to revoke consent or modify its preferences on cookies at any time, also through the mechanisms envisaged by the extended information notice. This notice should be linkable on every page of the website. Details are also given as to what the extended information notice should contain. For example, it should specify that users are allowed to express their choices regarding the use of cookies through browser

settings if the procedure to be followed to configure the settings is described. If technically possible, the website manager may also make a direct link available to the configuration section of the browser. This is different from many Member States who still feel that browser settings are not yet sophisticated enough. The Resolution does not clarify whether the extended information notice may be integrated into the website's privacy policy.

Use of profiling cookies is regarded by the Italian DPA as a profiling processing operation. Therefore, before placing a cookie, the relevant data controllers should file a specific notification with the Italian Data Protection Authority, or update any existing notification.

The Italian DPA recognises that compliance with these measures may encounter technical issues. Therefore, compliance is required at the latest by 2 June 2015 (one year after publication of the Resolution in the Italian Official Gazette).

LUXEMBOURG

In Luxembourg, the use of cookies is regulated by the act on data protection in electronic communications dated 30 May 2005 (the e-Privacy Act), as amended.

Pursuant to article 4(3)(e) of the e-Privacy Act, the use of cookies (including their storage on a subscriber's or user's device) is subject to the user's prior consent. Such consent must be free and based on clear and complete information, notably about the purposes of the processing. In this respect it should be noted that the Luxembourg e-Privacy Act remains subject to the requirements of the Luxembourg data protection act of 2 August 2002, as amended. For instance, there are further information obligations as well as specific restrictions for some acts of processing which may apply such as the non-occasional monitoring of the user's behaviour or movements carried out by technical means. Under the e-Privacy Act, a cookie is exempted from the informed consent requirement if it is necessary for the "storage or technical access for the sole purpose of carrying out the transmission of a communication over an electronic communications network" or if "it is strictly necessary for providers to provide an information society service explicitly requested by the subscriber or user". Generally, secure login, shopping basket and security cookies qualify as 'necessary' under the e-Privacy Act, and are therefore exempt from the consent obligation, as well as user interface customisation (such as setting the website language).

Where cookies are subject to the informed consent requirement, the Luxembourg legislator has explicitly accepted the possibility of consent being validly obtained through the user's browser or other application settings. However, the Article 29 Working Party's Opinion on cookie consent sets forth certain conditions which have to be fulfilled by browsers or any other application to be able to 'deliver' valid consent (such as where browser settings are predetermined to accept all cookies, this does not satisfy the consent requirement). Moreover, the Luxembourg data protection authority (the Commission nationale pour la protection des données) has in the past asked several Luxembourg based internet companies to display a banner or message about cookies at the top of their home page. It appears that it is acceptable that this message or banner is displayed only once, on a user's first visit, and need not be displayed on subsequent visits. Additional safeguards for users would be preferable such as requiring users to provide positive consent before cookies could be placed on their devices. Users must be given the clear and easy opportunity to oppose the use of cookies.

NETHERLANDS

In the Netherlands, the Telecommunications Act (Telecommunicatiewet) states that anyone seeking access through electronic communication networks to data stored in the terminal equipment of an end-user must (i) provide the user with clear and comprehensive information and (ii) obtain the user's unambiguous consent before being allowed to store information, or gain access to information already stored, on the user's terminal equipment.

As an exemption to this rule, consent is not required in respect of 'functional cookies'. These are cookies which are strictly necessary for communication purposes and/or for the correct functioning of services or webshops offered on websites. On 28 March 2014, a draft bill for a new Telecommunications Act was sent to Parliament which aims to extend the scope of this exemption. In respect of cookies that 'provide insight into the quality or effectiveness of service delivered via the internet and have little or no impact on the user's privacy', obtaining the consent of the user will no longer be required. Examples of these cookies are analytic cookies and affiliate cookies.

Regarding tracking cookies, the requirement to inform the user and obtain their consent before being allowed to store information, will remain in place. Tracking cookies are often used to analyse the behaviour of internet users or to draw up profiles.

The amended law has been submitted to Parliament and can enter into force after both legislative Chambers have approved the proposal. The legislation is expected to come into force at the end of 2014.

POLAND

Work on the new Polish regulations took longer than anticipated by the Revised Directive. The Revised Directive was finally implemented through an amendment to the Telecommunications Law, and the new "cookies regulation" became effective on 22 March 2013.

The national measures replaced the then current opt-out system with the obligation to receive consent to use cookies. Consent must be informed and must be given before data processing. However, consent can be given by a browser or application setting. As a result, the current system is a hybrid of the opt-out and opt-in models.

Although the law lacks more detailed regulations on this, commentators claim that consent does not need to be obtained each time the user enters a website and can cover particular categories of cookie (separate consent is not needed for each particular cookie). Further, it is not clear whether the lack of user activity and the use of default setting means that the user has granted his/her consent. There are views that it is acceptable if the set of information required by law is properly communicated. However, as the law clearly provides that consent cannot be implied from other legally recognised behaviours, this is debatable.

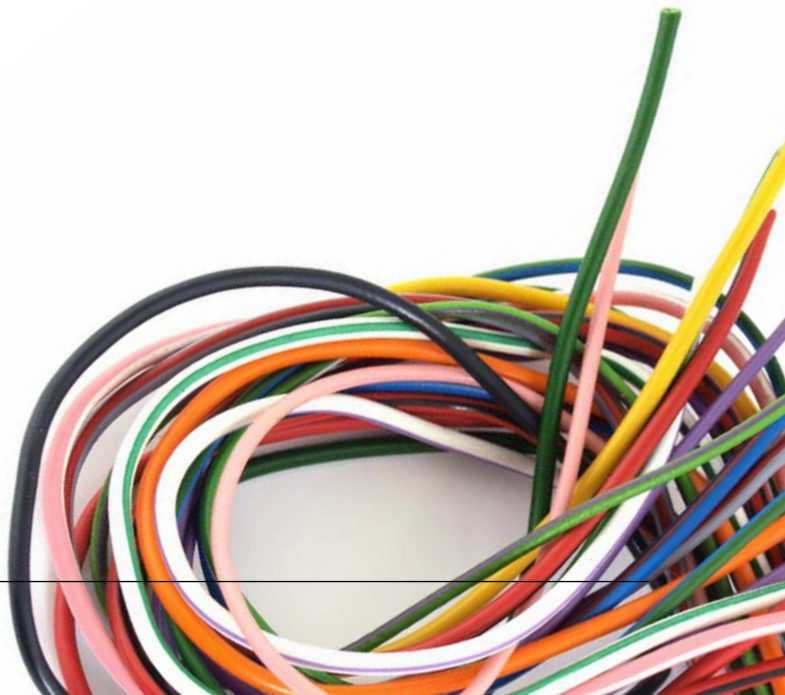
A common practice used by a number of service providers is to rely on default settings and have a pop up "cookie banner" at the top of the website with links to their cookie policy. Notably, it seems that a popular option is to have the cookie banner only the first time the user enters the website.

SPAIN

By Royal Decree 13/2012, the Information Society Services and E-Commerce Act in Spain was modified. Spain fully implemented the wording of the Revised Directive but imposed more restrictive criteria concerning users' consent expressed by browser settings or equivalent settings on other applications. The Spanish legislator initially incorporated Recital 66 to the Revised Directive (which states that the user's consent can be expressed by using the relevant settings of a browser where it is technically possible and effective) but added: "provided that the user proceeds to its configuration during its installation or update, or through an express action of the user to this purpose" and therefore limited the scope of Recital 66 following the criteria of the Working Party.

However, the adoption of the Spanish General Telecommunications Act 9/2014 on 10 May 2014 has modified the Information Society Services and E-Commerce Act further. Reference to the "express action of the user" has been removed and therefore browser settings are now considered sufficient to obtain users' consent.

The Spanish General Telecommunications Act also sets a penalty system empowering the Spanish Data Protection Authority to impose sanctions for failing to obtain users' prior consent or failing to provide sufficient information (the conduct is considered as a minor infringement, except in cases of recurrence). This penalty system also applies to advertising agents and networks when directly managing the placement of advertisements on websites if they fail to adopt sufficient measures to make the provider comply with its obligations to obtain consent and provide the required information.



UK

The Revised Directive was implemented in the UK through the Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2011 (SI 2011/1208) (the 2011 Regulations) which amended the Privacy and Electronic Communications Regulations 2003 (SI 2003/2426). The changes contained in the Revised Directive were copied into UK law by the 2011 Regulations and consequently the law allows for the use of cookies if informed consent is obtained. Following implementation, the Information Commissioner's Office (the ICO), the UK regulator, announced a grace period of 12 months during which it would not use its enforcement powers to allow for methods for compliance to be put in place.

The ICO published guidance on the use of cookies to assist websites with compliance. They suggest that companies should carry out a cookies audit to work out what they are using. They also state that the information that should be provided to users should be sufficiently full and intelligible to allow individuals to clearly understand the potential consequences of allowing the cookies should they wish to do so. It is necessary to be satisfied that the user understands that their actions will result in cookies being set.

Information only need be provided the first time a cookie is placed unless the purpose of the cookie being used later changes at which point the user must be informed of the changes and once again give their consent. "Consent" must involve some form of communication where the individual knowingly indicates their acceptance. Where possible, consent should be obtained prior to the use of cookies and where this is not possible, it should be obtained as soon as it can be. Explicit consent might be more appropriate if you are collecting sensitive personal data, such as health information.

While getting express prior opt-in consent does provide regulatory certainty, the most recent version of the ICO guidance specifically clarifies that implied consent is possible where there is some action taken by the consenting individual from which their consent can be inferred. The nature of the audience and their expectations will be relevant here. While some have seen this as a departure from other regulators, this is broadly in accordance with the views of many including the Working Party and the CNIL, as we have seen above.

A common current UK practice is to use a "cookie banner" at the top of a website which links to information on the site's use of cookies and in most cases contains a clickable box to indicate whether the user consents to those cookies. Where the user does not click to indicate their consent, the user can continue to use the site anyway and it may be implied that they have consented to the use of cookies by continuing to browse. Other methods used include the use of prominent links, clickable icons, pop-up windows and splash pages.

In relation to browser settings, the general view from the ICO is that it cannot be user consent where the browser allows cookies by default but it may be possible to give consent via browser settings should browsers become more sophisticated.

The International Chamber of Commerce published guidance in 2012 on the use of cookies. This contains a helpful description of various types of cookies. It also recommends universal adoption of standard notice and consent wording for each category used. We understand that the ICC are looking to update the 2012 guidance later this year but that they expect only minor changes will be made.

Have there been any consequences?

In many Member States it would seem that little has happened from an enforcement perspective. The ICO, for example, is still focussing on sites that have done nothing to try to comply or raise awareness of cookies. It has written to hundreds of companies asking them to take action to comply. The level of user concern about cookie consent on the internet which has been raised with the ICO has gone down markedly since 2012.

In January 2014, the Spanish Data Protection Authority (the AEPD) did fine two companies which had breached the Spanish requirements for cookie consent. They fined the two jewellery companies a total of EUR3,500 for not providing clear and comprehensive information about the tracking programs they used. A simple general legal notice was not held to be sufficient and it was made clear that the cookies used must correspond to the message provided. With the recently adopted General Telecommunications Act in Spain, these powers of the AEPD have been widened further (see above).

On 11 July the CNIL announced that it will be carrying out inspections to check whether companies are complying with its guidance on cookie consent. The CNIL have warned that they will use sanctions where companies are found to have failed to comply with French cookies law.

The AEPD fine and CNIL inspections show us that in some countries at least, the grace period for implementation is truly over.

What now?

Most Member States are now taking a pragmatic approach to the consent issue. We have certainly seen a common desire to avoid placing impractical burdens on websites and advertising network providers.

There are still concerns that the Revised Directive has been implemented inconsistently across EU Member States. As enforcement of the cookie consent requirements will be dealt with by the relevant national data protection authorities, this will inevitably lead to different approaches. However ANPs and website operators should also keep in mind the more comprehensive requirements as set out by the Working Party. We are certainly seeing a gradual shift towards a more aligned approach across many Member States.

It will be interesting to see whether the introduction of the proposed new data protection framework in the EU, in the form of the draft General Data Protection Regulation (GDPR), will have an effect on the way that we interpret cookie law. It is currently anticipated that the higher standard of consent required by the Revised Directive (and advocated by the Working Party) will continue to be followed.

After the initial reaction to the revised cookie consent requirements, perhaps the lesson we have learnt is that as long as the regulators and Working Party remain pragmatic in their approach to implementing and enforcing these pieces of EU-wide legislation, things are not always as bad as they at first appeared.

Your Allen & Overy contacts

UK

Jane Finlayson-Brown
Partner – Corporate
Tel +44 20 3088 3384
jane.finlayson-brown@allenovery.com

France

Ahmed Baladi
Partner – Corporate
Tel +33 14 006 53 42
ahmed.baladi@allenovery.com

Germany

Jens Matthes
Partner – Litigation
Tel +49 211 2806 7121
jens.matthes@allenovery.com

Italy

Lydia Mendola
Counsel – Litigation
Tel +39 02 2904 9713
lydia.mendola@allenovery.com

UK

Charlotte Mullarkey
Senior PSL – Corporate
Tel +44 20 3088 2404
charlotte.mullarkey@allenovery.com

UK

Nigel Parker
Senior Associate – Corporate
Tel +44 20 3088 3136
nigel.parker@allenovery.com

Belgium

Tom De Cordier
Counsel – Corporate
Tel +32 27 80 25 78
tom.decordier@allenovery.com

Netherlands

Quirine Tjeenk Willink
Counsel – Corporate
Tel +31 20 674 13 52
quirine.tjeenkwillink@allenovery.com

Poland

Magdalena Bartosik
Senior Associate – Corporate
Tel +48 22 820 61 31
magdalena.bartosik@allenovery.com

Spain

Victor Sagot
Associate – Corporate
Tel +34 91 782 98 00
victor.sagot@allenovery.com

Luxembourg

Gary Cywie
Counsel – Litigation
Tel +352 44 44 5 5203
gary.cywie@allenovery.com

GLOBAL PRESENCE

Allen & Overy is an international legal practice with approximately 5,000 people, including some 525 partners, working in 46 offices worldwide. Allen & Overy LLP or an affiliated undertaking has an office in each of:

Abu Dhabi
Amsterdam
Antwerp
Athens (representative office)
Bangkok
Barcelona
Beijing
Belfast
Bratislava
Brussels
Bucharest (associated office)
Budapest
Casablanca
Doha
Dubai
Düsseldorf
Frankfurt
Hamburg
Hanoi
Ho Chi Minh City
Hong Kong
Istanbul
Jakarta (associated office)
Johannesburg
London
Luxembourg
Madrid
Mannheim
Milan
Moscow
Munich
New York
Paris
Perth
Prague
Riyadh (associated office)
Rome
São Paulo
Shanghai
Singapore
Sydney
Tokyo
Toronto
Warsaw
Washington, D.C.
Yangon

Allen & Overy means Allen & Overy LLP and/or its affiliated undertakings. The term **partner** is used to refer to a member of Allen & Overy LLP or an employee or consultant with equivalent standing and qualifications or an individual with equivalent status in one of Allen & Overy LLP's affiliated undertakings.