STEPHENSON HARWOOD

Cookies

What are cookies?

Cookies are small text files that are downloaded onto an individual's device when that device is used to access a website. Cookies allow that device to be recognised and can be used to store certain information about an individual's preferences, activities and online and offline habits.

The rules that apply to cookies equally apply to any technology that stores or accesses information on an individual's device. This means that other similar technologies such as Local Shared Objects (sometimes called Flash cookies), scripts, apps on smartphones, tablets or other devices, tracking pixels, plugins, clear gifs and fingerprinting techniques are subject to the same laws and rules that apply to cookies.

For the purpose of this note, each of these technologies are referred to as "cookies".

What is the law on cookies?

The ePrivacy Directive (as implemented in the national law of the EU27 Member States and the United Kingdom) protects individuals from having information **placed on** their personal devices, or **accessed from** their devices, without their knowledge or consent. It applies to:

- The storage of any information on an individual's device or equipment.
- Access to any information already stored on the equipment. The same ePrivacy rules apply whether or not the information stored or accessed consists of, or contains, personal data.

Where cookies contain identifiers that may be used to target a specific individual, or where information derived from cookies may be used to target or profile individuals, this will also involve processing personal data. In these instances, the requirements of the EU General Data Protection Regulation 2016/679 (EU GDPR), the GDPR as it forms part of the domestic law of the United Kingdom by virtue of the European Union (Withdrawal) Act 2018 (UK GDPR) (for the purposes of this note, both the EU GDPR and the UK GDPR shall be referred to as the GDPR) and the UK Data Protection Act 2018 will also apply.

What do you need to do before using cookies?

The law requires those using cookies to do three things:

- Say that cookies will be used.
- Explain what those cookies will do and why.
- Obtain prior consent from each user to the use of cookies (unless an exemption applies, as set out below).

What is consent?

In this context, the standard for user consent is that imposed by the GDPR: this means a **freely given, specific, informed and unambiguous** indication of the individual's wishes by which she or he, by a statement or by a clear affirmative action, signifies agreement to the placing of cookies on a device. Consent must also be capable of being **withdrawn** at any time and as easily as it was given.

Exemptions to the requirement to obtain consent

The ePrivacy Directive offers two exemptions to the requirement to obtain prior consent in order to use cookies. These are:

The communications exemption

This applies to cookies used for the **sole purpose** of carrying out the **transmission of a communication** over a network.

The strictly necessary exemption

This applies to cookies that are strictly necessary to provide any service delivered over the internet (an "information society service"), such as a website or an app that has been requested by a user. Examples are:

- Load balancing cookies that ensure the content of your page loads quickly and effectively.
- Cookies used to remember what is in a user's basket on an internet shopping website.
- Cookies that provide security for the user's online session (such as those used for online banking services).

The guidance

This table examines the most recent guidance on cookies from three supervisory authorities in the United Kingdom, Ireland and France: the Information Commissioner's Office (ICO), Data Protection Commission (DPC) and Commission Nationale de l'informatique et des Libertés (CNIL).

<table>
<tr><th>Issues</th><th>ICO</th><th>DPC</th><th>CNIL</th></tr>
<tr><td colspan="4">Scope</td></tr>
<tr><td>Application of guidance</td><td colspan="3">Although the ICO, DPC and CNIL focus on cookies in their guidance, they are all clear that the guidance also applies to other similar technologies. In other words, the guidance from all three authorities applies to anyone who uses any method to store information on a user's device or gain access to information on a user's device.</td></tr>
<tr><td></td><td>The ICO's guidance applies to anything that stores or accesses information on a user's device. Examples given include: HTML5 local storage, Local Shared Objects and fingerprinting techniques.</td><td>The DPC's guidance applies to all tracking technologies such as local storage objects; 'flash' cookies, software development kits, pixel trackers (or pixel gifs), 'like' buttons and social sharing tools, and device fingerprinting technologies.</td><td>The CNIL guidance is particularly focused on the use of HTTP cookies but can apply to any operating systems or software applied to terminal equipment (as defined in the e-Privacy Directive).</td></tr>
<tr><td colspan="4">Consent</td></tr>
<tr><td>"Freely given" and "unambiguous": implied consent</td><td colspan="3">In accordance with the GDPR definition of consent, continued use of a website does not constitute valid consent, as it does not entail an affirmative action on the part of the individual to demonstrate agreement to the processing. Put simply, consent cannot be implied.

On 1 October 2019, the Court of Justice of the European Union (the "CJEU") delivered its judgment in Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband eV v Planet49 GmbH ("Planet49"), a case analysing the standard of transparency and consent for the use of cookies and similar technologies. A company called Planet49 ran a promotional lottery on its website. Upon entering the lottery, users were presented with two tick-boxes. The first was an unchecked tick box to receive third party advertising whilst the second was a pre-ticked box allowing Planet49 to set cookies to track the behaviour of users. Users were required to check the first box - agreeing to third party advertising - in order to enter the lottery.

Four key points arise from the Planet 49 judgment:
• Pre-ticked check-boxes authorising the use of cookies and similar technologies do not constitute valid consent.
• Where consent is required for cookies under the e-Privacy Directive, the GDPR standard of consent applies.
• It does not matter whether the cookies constitute personal data, the cookie consent rule applies regardless.
• Website users must be provided with information on the duration of the cookies, and whether third parties will have access to the cookies.

The impact of this case can be seen in the guidance from each authority but there are varying levels of practical advice given by the three different authorities.</td></tr>
<tr><td></td><td>The ICO is clear that silence or inactivity does not constitute consent. It follows that an end-user continuing to use a website does not imply valid consent.

This is very similar to the approach taken by both the DPC and CNIL.</td><td>The DPC states that assuming a user's consent based on their continued use of a website, is not permissible consent.

The DPC also specifies that scrolling cookie banners (i.e. banners that pop up when a user lands on a website but which subsequently disappear when a user scrolls, without any further engagement by the user) are also not compliant with the law.</td><td>CNIL considers that a user's silence, inaction or any action other than a clear positive act expressing their consent must be interpreted as a refusal to have cookies set on their devices.</td></tr>
</table>

Issues	ICO	DPC	CNIL
"Informed consent" and transparency of information	As mentioned above, the *Planet 49* case found that users must be provided with information on the duration of the cookies, and whether third parties will have access to the cookies.		
	The ICO states that any request for consent has to include the following information: • the cookies you intend to use • the purposes for which you intend to use them. The ICO makes clear that this information needs to be provided for cookies set by third parties as well as those set directly by the website owner. The ICO also advises that any consent request should include: • the name of your organisation • the name of any third party controllers who will rely on the consent • why you want the data • what you will do with it; and • that individuals can withdraw consent at any time.	Similarly, the DPC states that you must specify the purpose of each cookie as well as including a link or a means of accessing further information about your use of cookies and the third parties to whom data will be transferred when the user is prompted to accept the use of cookies.	The CNIL states that the following must be presented to users as a minimum before obtaining their consent: • the identity of the data controller(s) • the purpose of the data • how to accept or reject trackers • the consequences of refusing or accepting trackers • the existence of the right to withdraw consent.
"Specific consent": Global vs. Granular Consent	The consent must cover each purpose for which personal data will be processed (i.e. each purpose for which cookies are used). This raises questions as to whether prior contractual consent can be applied to all cookies or whether granular consent must be obtained. In other words, can consent for all cookies be obtained in a single affirmative action by a user?		
	The ICO recognises that consent must be clearly distinguishable from other matters and should be separate to any related contract or terms and conditions. ICO guidance states that separate granular consent options for separate purposes or types of processing should be given wherever possible.	The DPC recognises that you must not 'bundle' consent for cookies with consent for other purposes, or with terms and conditions for a contract for other services you are receiving. That said, the DPC does say that organisations can offer a global consent for all cookies for which consent is required in a first layer option. If this option is used, the second layer of information must provide more detailed information about the types and purposes of cookies being used and offer an option to opt in and out of each cookie.	In accordance with the ICO and DPC, the CNIL is clear that consent given as part of other terms and conditions is not valid consent. CNIL's position is that offering users a global consent to a set of purposes is possible, for example by using an 'accept all,' or 'refuse all' option, provided that users are notified in advance of all the purposes pursued, and there is the option for users to accept/reject each purpose. Requesting one consent for multiple cookies used for different purposes, without this granular option, may result in "consent bundling", which may render any consent obtained invalid. If a cookie has two purposes and consent is required for one of them, then consent must be obtained before deploying such a cookie (even if the other purpose falls into one of the exemptions and therefore doesn't require consent).

Issues	ICO	DPC	CNIL
Cookie walls	Cookie walls – sometimes called "tracking walls" – require users to agree to, or accept, the setting of cookies before they can access any online content. This is also known as the "take it or leave it approach".		
	The ICO considers that this approach is likely to be inappropriate, particularly if the use of a cookie wall is intended to require, or influence, users to agree to their personal data being used as a condition of accessing the service. This has the effect of taking away any genuine choice to use the service which goes against the requirement that consent must be freely given. However, the ICO also notes that this rule must be balanced with other rights such as freedom of expression and freedom to conduct business.	The DPC is silent as to the use of cookie walls but does specify that all consent must be freely given.	The CNIL no longer imposes a general and absolute ban on cookie walls but takes the position that they should be assessed on a case-by-case basis. However, CNIL considers that each service provider should clearly inform users about the consequence of accepting or refusing cookies when using a cookie wall. For example, users should be informed about the impossibility of accessing the service if they refuse cookies.
Refusal of consent: prominence of options	Each user must have the option to refuse consent to cookies. In providing this option, many service providers have historically used 'nudging' or incentives to encourage users to accept cookies rather than reject them. In the *Planet49* case, the CJEU noted that whilst the European Data Protection Board state in their guidance on consent that it is possible to incentivise consent to some extent, the onus remains on the controller to demonstrate that consent was freely given. This case, however, offers no guidance in respect to of when "nudging" prevents consent from being "freely given". The ICO, DPC and CNIL all ban "nudging" behaviours.		
	The ICO states that organisations emphasising the "agree"/"allow" cookie options, over the "reject"/"block" cookie options, are encouraging users toward the "accept" option. This kind of encouragement is not a compliant way to collect consent.	The DPC advises against the use of an interface that 'nudges' a user into accepting cookies over rejecting them. According to the DPC, if you use a button on the banner with an 'accept' option, you must give *equal prominence* to an option which allows the user to 'reject' cookies, or to one which allows them to manage cookies. The manage cookies option would then take users to a second layer of information in order to allow them to opt-in or out of cookies, by cookie type and purpose.	The CNIL emphasises that it must be as easy to accept the use of cookies as to refuse such use. Consent interfaces that only include "Accept All" and "Customize Settings" buttons, whereby users can accept all cookies by one click but may reject them via several clicks, are not lawful. If there is an "Accept All" button, there must be a "Reject All" button of the same size and at the same level on the interface. CNIL also advises that there should be an alternative interface that includes a link to allow users to continue without accepting. If selecting this option, it must be clear to users how they can reject cookies.

Issues	ICO	DPC	CNIL
Withdrawal of consent	Consent must be able to be withdrawn as easily as it is given. This means that users must always have an accessible option to withdraw consent made available to them.		
	The ICO requires website operators to provide information about how consent can be withdrawn, and how cookies that have already been set can be removed within the consent mechanism.	The DPC mirrors the ICO in advising website operators to provide information about how users can give, and later withdraw, their consent to the use of cookies, including by providing information on the action required for them to signal such a preference.	The CNIL gives a more detailed insight as to how the right to withdraw consent should be notified to users. Some key points are: • users must be informed in a simple and intelligible manner • information must be available before consent is given • the mechanism for withdrawing consent should be offered via a link accessible at any time from the service concerned with a descriptive and intuitive name, such as 'management module of cookies' or 'manage my cookies' or 'cookie.'
Third party cookies			
Analytics cookies: first party and third party	Analytics cookies are used by online service providers to collect information about how people access their services – for example, the number of users on a website, how long they stay on the site for, and what parts of the site they visit. The fact that analytics cookies require consent is recognised by all three authorities but some questions are raised about the likelihood of enforcement action.		
	According to the ICO, analytics cookies do not fall within the "strictly necessary" exemption. This means service providers need to tell people about analytics cookies and obtain consent for their use. Although the ICO does not rule out the possibility of enforcement action in any area, it has stated that it will take a risk-based approach to enforcement where the setting of a first-party analytics cookie without consent results in a low level of intrusiveness and low risk of harm to individuals.	The DPC takes the view that consent is required for all analytics cookies. However, the DPC also notes that it is unlikely that first-party analytics cookies would be considered a priority for enforcement action by the DPC (mirroring the opinion shared by the ICO).	The CNIL has historically considered that analytics cookies could be exempt from the consent requirement, subject to strict conditions, which include the ability for users to opt out of having such cookies. As a result, very few analytics solutions could, in practice, benefit from the consent exemption. The CNIL has now softened these conditions. The consent exemption only applies to analytics cookies whose purpose is limited to measuring the audience of the website or app on behalf of the website publisher (i.e. first party analytics cookies measuring website business). These analytics cookies must be used solely to produce anonymous statistics, and the personal data collected through the cookies must not be combined with other data or processing activities and must not be shared with third parties.

Issues	ICO	DPC	CNIL
Joint controllers: third party cookies	Cookies may be either first party or third party cookies. In general, a cookie set by your own website, i.e. the host domain, is a first party cookie. A third party cookie is one set by a domain other than the one the user is visiting, i.e. a domain other than the one user sees in their address bar. The setting of third party cookies raises the question about who is responsible for these third party cookies. On 29 July 2019, the CJEU issued its judgment in a case called *Fashion ID GmbH & Co.KG v Verbraucherzentrale NRW eV* ("**Fashion ID**"). This case concerned a Facebook "Like" button that had been placed the website of an online fashion shop (Fashion ID). This resulted in the transmission of user data to Facebook's server when the user accessed the website. The transfer of data happened without the user's knowledge, and occurred regardless of whether the user had a Facebook profile or if the user actually clicked the "like" button. Two questions arose for the CJEU: • If a website operator embeds a social plugin or cookie from which user data is transferred to the provider of that plugin or cookie, is the website operator a joint controller regardless of its limited role in processing the data? • If they are a joint controller, which one of the joint controllers (the website operator or the plugin owner) is responsible for providing information to, and collecting consent from, the website visitor?		
	The CJEU held that the website operator can qualify as a controller, jointly with a social plugin provider. Consequently, the website operator is directly responsible for complying with its legal obligations as a controller, including informing its users that their personal data will be transferred to the third party plugin provider. This means that website operators also need to ensure that users give their consent to the use of any third party plugin. However, the CJEU importantly clarified that the website operator's role as a controller (and its corresponding legal obligations) is limited to the collection and transmission of the data to the third party plugin provider and does not include any subsequent personal data processing carried out by that third party.		
	The ICO considers the practicality of being a joint controller, recognising that it is more difficult for third party cookie providers to ensure consent is obtained accurately and legally, as they have less control over the consent interface. In order to protect the position of third party providers, the ICO advises that the joint controllers enter into a contract with terms setting out the interface requirements.	The DPC simply makes the point that website operators should be aware of any third party cookies and the fact that they might be considered a controller. This is less explicit than the ICO and CNIL guidance and does not offer any practical guidance.	Following the Fashion ID case, the CNIL made clear that the body which authorises the use of cookies, including by third parties, from its website or mobile application, must ensure there is an effective mechanism in place for obtaining user consent. In doing so, the CNIL clarifies that a website owner remains liable for third party cookies even when it subcontracts the management of cookies to another party.

Issues	ICO	DPC	CNIL
Retention			
Cookie lifespan	The ICO suggests that the length of time for which you use any cookie must be proportionate to the outcome intended of the use of the cookie, and limited to what is necessary to achieve your purpose. For example, use of a persistent cookie (i.e. a cookie stored on a device which is set to expire at some future time), rather than a session cookie (being a cookie that expires when a browser is closed) would need to be justified on the basis that the cookie's functionality necessarily requires it to be persistent.	The DPC states that the lifespan of a cookie must be proportionate to its function. It states that, for example, it would not be proportionate to have a cookie with a lifespan of 'forever'.	The CNIL prescribes lifespans for analytics cookies but does not indicate a specific lifespan requirement for other cookies.
Re-requesting consent	According to the ICO, there is a range of reasons why you may need visitors to "re-consent" to cookies. However, depending on the circumstances you may not need to ask for fresh consent each time someone visits. The ICO says that an example of where you need to obtain fresh consent is when you are setting non-essential cookies from a new third party. The ICO also notes the importance of deciding an appropriate interval between when you require users to select their preference and when users may be given the option to indicate their preferences again.	The DPC states that six months is an appropriate default timeframe for storing users' data, including their consent preferences. The DPC notes that a controller would need to justify any longer storage period objectively and on a case-by-case basis.	When consent is given and recorded, the CNIL recommends renewing the consent obtained at appropriate intervals. The CNIL notes the importance of recording a refusal to consent (as well as any consent) in order to avoid requesting new consents from those users who have previously refused, which may pressure or influence a user's decision.

Contact

Katie Hewson

Partner

T: +44 20 7809 2374
E: katie.hewson@shlegal.com

Olivia Fraser

Associate

T: +44 20 7809 2844
E: olivia.fraser@shlegal.com

Sarah Bryant

Associate

T: +44 20 7809 2206
E: sarah.bryant@shlegal.com

Stephenson Harwood is a law firm with over 1100 people worldwide, including more than 180 partners. Our people are committed to achieving the goals of our clients – listed and private companies, institutions and individuals.

We assemble teams of bright thinkers to match our clients' needs and give the right advice from the right person at the right time. Dedicating the highest calibre of legal talent to overcome the most complex issues, we deliver pragmatic, expert advice that is set squarely in the real world.

Our headquarters are in London, with nine offices across Asia, Europe and the Middle East. In addition we have forged close ties with other high quality law firms. This diverse mix of expertise and culture results in a combination of deep local insight and the capability to provide a seamless international service.

www.shlegal.com

STEPHENSON HARWOOD

BD1216-Cookies guidance-0721