HFN Technology & Regulation Special Client Update:

Practical Cookie Consent Handbook [updated: July, 2019]

Introduction

This handbook was prepared to help businesses operating in the digital ecosystem – such as publishers, mobile app developers, ad networks and agencies, analytics/attribution providers, fraud prevention tools, and others – identify and meet the key requirements that apply to the storing of information, or otherwise gaining access to information stored, on a device, as well as to locate resources and tools that may help them meet these requirements.

Why are these guidelines important?

If you operate a website or app, you probably use cookies or similar tracking technologies in order to offer your visitors a better user experience, to understand what kinds of visitors use your service, and to show them relevant ads.

Common examples include:

- A retail website that uses cookies to remember the visitor's shopping preferences;
- A blog that uses an analytics provider that uses cookies to capture aggregate demographic information and analyze traffic;
- A news media website or gaming app that uses a third-party ad server to track users' browsing behavior and display targeted ads;
- A website that installs a social platform pixel or plug-in in order to measure ad conversions or retarget advertisements on such social platform.

Following the application of the General Data Protection Regulations ("**GDPR**"), the Directive 2009/136/EC ("**e-Privacy Directive**") has created obligations to provide notice and obtain consent from visitors for the use of tracking technologies, particularly where these enable the collection of personal data (such as IP addresses or persistent device identifiers).

It is expected that data protection authorities across the EU will enhance their efforts to scrutinize websites and enforce these new guidelines, basing on a risk-based approach and in line with their respective regulatory action policy.

To what activities these guidelines apply?

These guidelines apply to **any activity that involves storing of information on an end user's device, or otherwise gaining access to information on an end user's device,** via various tracking technologies. The guidelines do not apply to any prior or subsequent processing operations involving this information.

Note that these guidelines use the single term 'cookies' to refer to cookies and all other similar technologies, including: SDKs, scripts (such as JavaScript), tracking pixels, plugins, HTML5 local storage, Local Shared Objects (sometimes called Flash cookies), device fingerprinting (i.e. combining a set of information elements in order to uniquely identify a particular device), and other forms of local storage or tracking technologies.

These guidelines are relevant to **all types of digital properties, both websites and mobile applications alike**.

Further, **these guidelines apply regardless if the data that is stored or accessed via the cookies constitutes personal data (e.g. IP addresses)**.

What do these guidelines include?

These guidelines include the following:

1. What are the **key requirements for the use of cookies**?
2. **Detailed explanation of the notice and consent requirements**, together with visual examples of non-complaint behaviors.
3. **Overview of scenarios when the consent requirement does not apply**, together with common examples (see Exhibit).
4. **Practical takeaways** for:
   a. First parties (e.g. publishers, website operators, mobile app developers);
   b. Third parties (e.g. analytics providers, tracking/attribution providers, media players streaming service, ad networks, SSPs/DSPs, fraud prevention tool, etc.).
   c. Third party designing and developing websites or similar technologies for others.

What are the key requirements for the use of cookies?

This activity is subject to two key rules:

1. **Notice**: the users should be notified that cookies or other tracking technologies are being used, and should be informed what the cookies are doing, and why.

   AND

2. **Consent**: the users should provide their consent to store the cookies or other tracking technologies on their devices. This requirement has certain exemptions, discussed below.

Both requirements will be discussed below.

What is the "notice" requirement?

What does it mean?

User must be provided with clear, easily available and comprehensive information regarding the use of cookies, explaining the way the cookies work and what they are used for, enabling users to understand the potential consequences of allowing the cookies.

What the notice should include?

The notice should include all of the following information:

1. Type of cookies – whether they are "first party" cookies (set directly by the website the user is visiting, i.e. the URL displayed in the browser's address bar), or "third party" cookies (set by a domain other than the one the user is visiting).

2. Purpose of cookies – cookies can be used for a variety of purposes, including analytics, audience measurement and segmentation, remembering user's preferences, ad targeting, authentication and security purposes.

3. Duration/lifespan of cookies – whether they are "session" cookies (cookies that expire at the end of a browser session, typically when a user exits their browser) or "persistent" cookies (cookies that can be stored for longer, in which case its expiry is set by the website operator), and their lifespan/expiry date.

4. Identify all third parties – the notice should not include ambiguous or unclear references to 'partners' or 'third parties', but specify all the vendors involved in the context of the cookies' deployment, with links to their respective privacy policies.

5. Settings/opt-out – how individuals are able to opt-out of the use of cookies.

How the notice should be formatted?

A notice can be formatted in a variety of ways, including banners, pop-ups, message bars, header bars or 'splash pages'. The notice should meet the following requirements:

1. **Prominence and positioning** – information should be provided in such a way that the users will see it when they first visit your website or app.

   A notice cannot be provided as part of a privacy policy that is hard to find – the notice must be **visible and prominent** (e.g. via a "sticky" and "above the fold" notice on the website).

   More detailed information about cookies should be provided, either through the consent mechanism discussed below, or in a cookie policy accessed through a link within the consent mechanism and at the top or bottom of your website.

2. **Formatting** – the size, color or font of the link to the information should be distinguishable from "normal text" and other links.

3. **Wording** – the link should be more than simply "privacy policy"; this could involve a link through some explanatory text (e.g. "Find out more about how our site works and how we put you in control").

What is the "consent" requirement?

What does it mean?

Excluding specific scenarios discussed below **– valid and affirmative consent is always required when using cookies**.

To be valid, consent must be **freely given, specific and informed**, and must involve a **form of a clear positive action** – for example, ticking a box or clicking a button or a link.

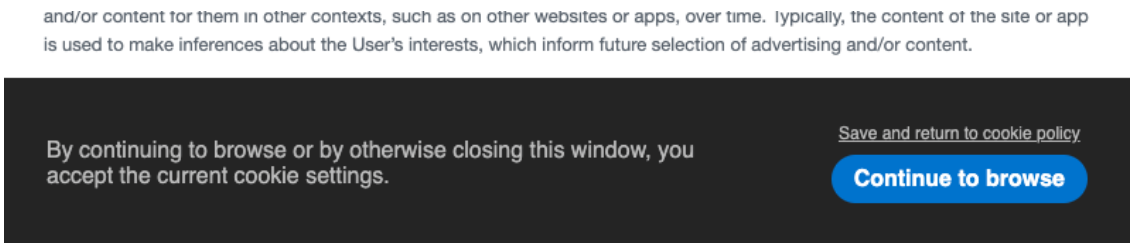
This means that the alternative lawful grounds provided under the GDPR (e.g. "legitimate interest") can no longer be relied upon, whether or not personal data is collected.

What behaviors do not comply with the consent requirement?

1. **No "soft opt-in" – consent must be given by a clear and deliberate positive action** (such as by engaging with the consent box or the options available within).

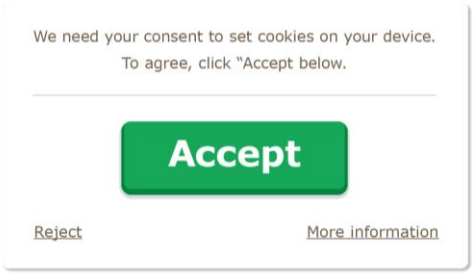
   Statements such as 'by continuing to use this website you are agreeing to cookies', pre-ticked boxes or any equivalents, such as sliders defaulted to 'on', should not be used (even if the banner also includes an 'OK' or 'Accept' button).

Example for non-compliant behavior



2. **No "nudge" techniques** – a consent mechanism should not be designed in a way that influences the users towards the 'accept' option, e.g. by emphasizing 'agree' or 'allow' over 'reject' or 'block'.

Example for non-compliant behavior



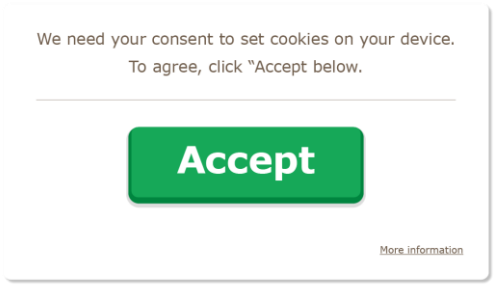
3. **Easy controls/means to disable** – users should have **easy means** to enable or disable cookies. This effectively means that providing instructions to users to disable cookies via the browser's settings is unlikely to be considered compliant.

   It cannot be assumed that a visitor can configure their browser settings to correctly reflect their preferences in relation to the setting of cookies.

   Further, implementing a consent mechanism that works only for some of the cookies would not be compliant – users should not be required to visit different websites and take different actions to disable them.

4. **No cookie walls** – the use of "cookie walls" to restrict access to a website until users consent will not comply

Example for non-compliant behavior



5. **Record consent** – consent must be demonstrated, meaning that the visitor's consent and withdraw (opt-out) request should be captured, including by recording the User ID and timestamps. Mere presence of a contractual requirement to obtain consent is not sufficient.

6. **No "bundling"** – users must be able to give consent independently and specifically for each separate purpose. Providing the user with the opportunity to consent in a comprehensive manner is acceptable, provided that this is in addition to, but not substituted for, the possibility of specifically consenting to each purpose.

When is consent not required?

Consent is not required **only in the following two scenarios**:

1. **Communication** – the cookie is for the sole purpose of carrying out the transmission of a communication over an electronic communications network.

   This applies for cookies used for routing information over a network by identifying the communication 'endpoints' (devices that accept communications across that network), exchanging data items in their intended order, or detecting transmission errors or data loss.

   OR

2. **Strictly necessary** – the cookie is strictly necessary to provide a service over the internet, which is requested by the user.

   Note that it must be essential to fulfill the user's request – cookies that are helpful or convenient but not essential, or that are only essential for your own purposes, will still require consent.

This also applies to cookies comply with any other legislation that applies to you, for example, the security requirements of data protection law.

In the Exhibit to these guidelines you will find common examples of when consent is not required, as well as examples of when consent is required. Please note these are indicative and not exhaustive lists.

Practical Takeaways

For first parties

If you are a first party (e.g. a website operator or mobile app developer) –

1. **Conduct a cookie audit –** this means you should take steps to identify and document what cookies you are using. You can perform this through a combination of browser-based tools and server-side code review. The audit should include:
   i. the purpose(s) of each of the cookies you use (or intend to use);
   ii. what data is processed through the cookies, including personal data;
   iii. the type of cookie – first party or third party (and who is setting the cookie);
   iv. the duration of the cookie – session or persistent.

2. Confirm the cookies are justifiable, including that their lifespans are justifiable for the stated purpose.

3. **Identify cookies that are exempt from the consent requirement**

4. **Implement an adequate consent and notice mechanism –** ensure that your notice and consent mechanism meets the requirements discussed above (e.g. no "nudge techniques", no "cookie walls", providing sufficient and comprehensive information, enabling users to control the setting of all cookies).

   Stay informed of industry developments! Consider a consent management platform ("**CMP**") based on the IAB Transparency and Consent Framework, Version 2.0 ("**TCF**").

5. **Periodically review your use of cookies** – review your use of cookies on a periodical basis, including obtaining new consent when the cookie has expired or when setting cookies from a new third party.

For third parties

If you are a third party (e.g. analytics provider, tracking/attribution provider, media players streaming service, ad network, fraud prevention tool, etc.) wanting to set cookies through others, we recommend the following steps–

1. **Contracts** – you should include a contractual obligation into your agreements with web publishers. This can provide assurance that appropriate steps will be taken to provide information about the third party cookies and to obtain consent.

2. **Support industry standards** – You should consider registering as a vendor with an industry accepted consent framework, such as an IAB Global Vendor of the IAB TCF, thereby supporting your clients who elect to implement industry accepted consent mechanisms.

3. **Audit/monitoring** – You should consider taking further steps, such as ensuring that the consents were validly obtained.

4. **Consider providing your own CMP** – you can consider designing and providing your own consent mechanism or consent management protocol.

5. **Education** – you should consider educating your clients about the importance of implementing these requirements (e.g. via marketing materials/webinars).

If you are a third party designing and developing websites or similar technologies for others –

1. You must consider the requirements herein and make sure the systems you design allow your clients to comply with the law.

2. You must also ensure that when you design and develop new online services, or upgrade software, that you take into account these requirements.

EXHIBIT – WHEN IS CONSENT NOT REQUIRED? COMMON EXAMPLES

Common examples where consent is not required

PURPOSE	DESCRIPTION OF ACTIVITY
User input	Using session cookies to track user input for specific functions of your service (e.g. a shopping basket or completing a form).
Authentication	Using first-party session cookies for authentication purposes. However, this does not apply to persistent login cookies.
Security	Using first-party cookies to detect authentication abuses, for fraud prevention, to detect repeated failed login attempts, or to comply with data protection security requirements for an online service the user has requested (e.g. online banking services), provided that the cookies are linked to the functionality explicitly requested by the user. However, this does not apply to cookies that relate to third party security requirements.
Streaming content	If your service is an online content provider that uses session cookies in the context of streaming media (such as flash player cookies). This does not apply to personalization or usage monitoring. However, this may not apply to online services that merely include streaming content hosted by a third-party online content provider (e.g., where a website embeds YouTube videos, even those from its own YouTube channel),
Network management	Using session cookies for load balancing purposes (i.e. for ensuring that the content of the page loads quickly and effectively by distributing the workload across several computers. This applies only where the cookies are for the sole purpose of identifying which server in the pool the communication will be directed to.
User preference	Using session cookies to store a user's preference (such as to optimize the site's layout, or using responsive design, so that the site changes depending on the type of device), provided they are not linked to a persistent identifier. In some cases, this may also apply to persistent cookies.
Social media plugins	Where a user of your online service is also logged in to a social media platform, and your service includes plugins and other tools provided by that platform that are necessary as part of the users' interaction with the social network. **The plugins must be configured to set cookies on devices used by logged-in members of the social media platform**.

Common examples where consent is required

PURPOSE	DESCRIPTION OF ACTIVITY
Social media plugins	Where a user of your online service is not logged to the social media platform – e.g. users who have logged out, or users that are not members of that network.
Social media tracking	Where a social media plugin or other technology tracks users, whether or not the users are members of that particular platform, for other purposes (e.g. online advertising, behavioral monitoring, analytics, or market research).
Advertising, personalization and data-brokering	If your service includes cookies used for the purposes of online advertising, personalization and data brokering. This includes all third-party cookies used in online advertising, including those used for operational purposes related to third-party advertising, such as frequency capping, ad affiliation, click fraud detection, market research, product improvement, debugging and any other purpose.
Cross-device tracking	Where you use cookies to link a user's account with a particular device or devices (e.g., as part of the account profile, to provide a second authentication factor or to track users across multiple devices for any purpose – including advertising).
Analytics and audience measurement	Certain regulators adopted the view that any type of analytics cookies, such as those used to collect information about how visitors access your site/app (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) – require consent. However, this approach differs, with certain regulators adopting the view that audience measurements and segmentation, which does not involve cross-site tracking and which is confined to the production of anonymous statistics, may be excluded from the consent requirement.