

The Ultimate Cookie Handbook for Privacy Professionals

January 4, 2018

Disclaimer

No part of this document may be reproduced in any form without the written permission of the copyright owner.

The contents of this document are subject to revision without notice due to continued progress in methodology, design, and manufacturing. OneTrust LLC shall have no liability for any error or damage of any kind resulting from the use of this document.

OneTrust products, content and materials are for informational purposes only and not for the purpose of providing legal advice. You should contact your attorney to obtain advice with respect to any particular issue. OneTrust materials do not guarantee compliance with applicable laws and regulations.

Table of Contents

Table of Contents	2
Part 1: Understanding the Terminology and Requirements	3
Terminology	4
What are Cookies?	4
What are cookies used for?	4
What are the different types of cookies?	5
Other Tracking Technologies	5
Requirements	7
The e-Privacy Directive	7
Consent: the only legal basis available for cookies	7
Some cookies are exempt from the consent requirement	7
The Directive created a fragmented landscape in the EU	8
GDPR	8
The GDPR and Cookies	9
The GDPR and Consent.....	9
Approaches to consent.....	10
The Draft e-Privacy Regulation	11
Cookies in the Consultation.....	12
Significant Opinions	12
What are the changes for cookies brought by the draft e-Privacy Regulation?.....	14
Conflicts and Uncertainties for Site Owners	17
Part 2: Operationalizing cookie requirements and best practices	18
Tips from the EU Commission for lawful cookie use	18
Cookie notice/policy	18
Cookie Compliance tools available	19
EU Commission Cookie Consent Kit.....	19
CNIL How to Guide for websites, cookies and other tracking technologies	19
OneTrust Cookie Compliance	20
Part 3: Additional resources	22
About OneTrust	23

Part 1: Understanding the Terminology and Requirements

Terminology

What are Cookies?

A cookie is a small piece of data (text file) that a website – when visited by a user - asks your browser to store on your computer or mobile device in order to remember information about you¹, such as your language preference or login information.

All cookies are browser specific. For example, if you use Internet Explorer, visit a website and select “French” as your preferred language, a cookie may be placed on your computer so that when you visit this website in the future, it will know to display it in French. However, if the next time you visit that same website, you use Chrome instead of Internet Explorer, the site will not know that you prefer seeing it in French.

Cookies are not good or bad, they are just a tool that can be used to do different things.

What are cookies used for?

Cookies are enabled by the owner of a website. Originally, they were created to enable e-commerce solution for the web, as the web did not have any concept of memory. Today, they are meant to enhance the overall experience of a person visiting a website.

For example, websites use cookies to:²

- Identify users
- Remember users' custom preferences (such as language preference)
- Help users complete tasks without having to re-enter information when browsing from one page to another or when visiting the site later
 - Browsing from one page to another: For example, when online shopping, a cookie is what allows a visitor to select an item to purchase and seeing this item again when they click and are directed to the “Check-out” page
 - When visiting the site later: For example, when you enter your e-mail address and password and click “remember me” so that when you visit the site again, your e-mail address and password will already be “pre-typed”

All those cookies are set by the owner of the website and are called first party cookies. Only the particular website you visited will know and remember some information it gathered about you while you were browsing the website.

But, cookies can also be used by search engines and online advertisers for online behavioural target advertising. A third party cookie is a cookie that does not originate from the website that you are visiting. It is placed on a user’s hard disk by a web site from a domain other than the one you are visiting. They are often set by advertising networks that a site may subscribe to in the hopes of driving up sales or page hits.³ They are also sent by advertisers, which embed

¹ http://ec.europa.eu/ipg/basics/legal/cookies/index_en.htm

² http://ec.europa.eu/ipg/basics/legal/cookies/index_en.htm

³ <http://whatis.techtarget.com/definition/third-party-cookie>

“piece” of their website in someone else’s website, which allows them to store a cookie on your machine as well. For example, if you visit a news website and the site has a couple ads on it. The news website itself can store cookies on your device (first party cookies) but your browser is also communicating with another website – which is the website that has the ad that is displayed on the news website. That other website can also store a cookie on your device, which will be a third party cookie.

What are the different types of cookies?

A cookie can be classified by its lifespan and the domain to which it belongs. By lifespan, a cookie is either a:⁴

- **session or temporary cookie** which is erased when the user closes the browser *or*
- **persistent cookie** which remains on the user's computer/device for a pre-defined period of time.

As for the domain to which it belongs, there are either:⁵

- **first-party cookies** which are set by the web server of the visited page and share the same domain
- **third-party cookies** stored by a different domain to the visited page's domain. This can happen when the webpage references a file, such as JavaScript, located outside its domain.

There are other, more controversial, types of cookies, such as Flash cookies. Flash cookies are an example of tracking methods that are less noticeable and harder to remove. Flash cookies are cookies that reappear or “respawn” after deletion. It is a standard HTTP cookie backed up by data stored in additional files that are used to rebuild the original cookie when the user visits the originating site again⁶. They are stored in a different place on your device or online, which means that they are not deleted when you delete your browser cookies.

Other Tracking Technologies

Historically, techniques for tracking and storing people’s preferences on the web have relied on HTTP cookies – small text files that ‘tag’ a person’s browser so it can be uniquely identified. Cookies are one of the ways to track users but many other similar technologies exist.

For example, web beacons (also called web bugs or pixel tags) are often-transparent graphic image, usually no larger than 1 pixel x 1 pixel, that is placed on a Web site or in an email and is used to monitor the behavior of the user visiting the website or sending the email. The technology is often used in combination with cookies.⁷ Web beacons allow companies and online marketing agencies, for example, to know if readers are opening the html emails they receive. When the Web beacon loads (which happens when the email is opened), the Web beacon is embedded invisibly in the email graphics, so the company can find out if the recipient opened the email, when it was opened. It can also help gather information such as the IP address of the computer, the URL of the web page the bug is located on, the URL of

⁴ http://ec.europa.eu/ipg/basics/legal/cookies/index_en.htm

⁵ http://ec.europa.eu/ipg/basics/legal/cookies/index_en.htm

⁶ <http://whatis.techtarget.com/definition/respawning-cookie>

⁷ https://www.webopedia.com/TERM/W/Web_beacon.html

the page the bug came from, the time the bug was observed, a set cookie value, the type of browser that was used to get web bug graphic image.⁸

Browser fingerprinting is another technique allowing to identify web users by collecting information about a remote device. The technology can identify a user even when cookies are turned off.

Although this handbook focuses on cookies, the e-Privacy Directive and future e-Privacy Regulation apply to anyone who stores information on a user's device, which means it applies to any similar technologies (such as Local Shared Objects) and any terminal equipment (laptop, smartphone, tablet, smart TV or other similar devices). The draft e-Privacy Regulation (addressed below in more details) covers all types of tracking technologies and none of these tracking techniques would be allowed without the user's consent.

⁸ <http://whatismyipaddress.com/web-beacon>

Requirements

The e-Privacy Directive

Current requirements for cookies in Europe are derived from the ePrivacy Directive⁹ (ePD), the current version of which came into effect in 2011. Because the requirements are set forth in a Directive, it requires each Member State to transpose them into national law.

The ePrivacy Directive (ePD) was first introduced in 2002, and revised in 2009. It is primarily concerned with the confidentiality of electronic communications, and many of its requirements cover telecommunications companies.

Consent: the only legal basis available for cookies

Article 5(3) of the e-Privacy Directive, requires, in short, that any “storing or retrieving” of information from an end users’ device be subject to consent unless it is technically necessary to enable the intended communication to take place.

Note that this requirement may cover a wide range of circumstances, and applies to a range of different technologies and techniques for storing and retrieving information from a user’s device (so called “terminal equipment”).

Web cookies are the most common technology to be directly impacted by the consent rule. It is the requirement for cookie consent that has given rise to the use of various cookie notification banners and pop-ups found on many websites.

Whether the cookies involve personal data, or represent any kind of privacy risk to the user, is not relevant to this requirement.

Additionally, because cookies are stored on the end-user terminal equipment, both first party and third party cookies are covered by the rule. Consent needs to be given for all types of cookies when a user land on a particular webpage and the website publisher is the person responsible for collecting the user’s consent (whether the cookie is a first party cookie or a third party cookie).

Some cookies are exempt from the consent requirement

The **only allowable exception** is when the use of the cookies is “strictly necessary” for the operation of the site. Exemptions allowed under this rule are quite narrow.

Consent is not required if the cookie is:

- used for the sole purpose of carrying out the transmission of a communication, and
- strictly necessary in order for the provider of an information society service explicitly required by the user to provide that service.

⁹ <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32002L0058&from=FR>

Cookies clearly exempt from consent according to the EU advisory body on data protection- WP29¹⁰ include:

- **user-input** cookies (session-id) such as first-party cookies to keep track of the user's input when filling online forms, shopping carts, etc., for the duration of a session or persistent cookies limited to a few hours in some cases
- **authentication** cookies, to identify the user once he has logged in, for the duration of a session
- **user-centric security** cookies, used to detect authentication abuses, for a limited persistent duration
- **multimedia content player** cookies, used to store technical data to play back video or audio content, for the duration of a session
- **load-balancing** cookies, for the duration of session
- **user-interface customisation** cookies such as language or font preferences, for the duration of a session (or slightly longer)
- **third-party social plug-in content-sharing** cookies, for logged-in members of a social network.

It is also important to note that outside the necessity exemption, consent is the only legal basis for setting cookies, which is a big difference with wider data protection and privacy laws in general, such as the upcoming General Data Protection Regulation, which allows for additional legal grounds for processing (like legitimate interest, or necessary for the performance of a contract)

The Directive created a fragmented landscape in the EU

One of the key difficulties with the ePD was that its requirements had to be written into national law in each EU Member State, which sets it apart from a Regulation like the GDPR. This has created quite a lot of variation in interpretation.

National regulators have also put out their own guidance interpreting the rules around cookies differently, including when and how consent can be obtained/given, as well as what kinds of cookies might fall under the exemption for consent.

Regulators also have widely differing powers and approaches to enforcement. As a result, cookie notices in the UK, France, the Netherlands, and Italy, for example, greatly vary in both content and functionality. The same website with the same cookies, but serving different national markets, can vary in what information and options are given to users.

The situation is both complicated for website owners and confusing for end-users, who find themselves presented with a broad range of choices on the websites they visit, and often no real choices at all. For businesses that operate in multiple countries in the EU, attempts to comply with the letter of the law can bring many challenges, and when there's a low chance of regulation enforcement, there's a good chance that companies will do as little as possible to comply.

GDPR

The EU's General Data Protection Regulation (GDPR) was passed in May 2016 and will enter into force on 25 May 2018. Regulations and Directives are the two possible ways to pass legislation in the European Union. But directives require each member state to pass a national law implementing the requirements of the directive (creating discrepancies

¹⁰ http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp194_en.pdf

between Member States) while regulations are directly applicable in each member state. The goal of using a regulation for the reform was to harmonize the data protection framework across the European Union.

While the ePrivacy Directive ensures the protection of fundamental rights and freedoms, in particular the respect for private life, confidentiality of communications and the protection of personal data in the electronic communications sector, it also guarantees the free movement of electronic communications data, equipment and services in the Union. It implements in the Union's secondary law the fundamental right to the respect for private life, with regard to communications. The GDPR covers all matters concerning the processing of personal data not specifically addressed in the ePD or future e-Privacy Regulation.¹¹

The GDPR and Cookies

Recitals in the GDPR make it clear that some types of cookies will, by their nature, involve processing of personal data. There are 2 recitals that are key to this:

Recital 30

Natural persons may be associated with online identifiers...such as internet protocol addresses, cookie identifiers or other identifiers. This may leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them.

This tells us that cookies which are used to uniquely identify the device and/or the individual associated with using the device, should be treated as personal data.

This position is also reinforced by Recital 26, which states that personal data is also defined by data that can reasonably be used, either alone or in conjunction with other data to single out an individual or otherwise identify them indirectly. Use of pseudonymous identifiers (e.g. strings of numbers or letters,) which is what cookies often contain to give them uniqueness, also qualifies as personal data, so under the GDPR, any cookie or other identifier that is uniquely attributed to a device or user and therefore capable of identifying an individual, or treating them as unique even without actually identifying them, counts as processing of personal data.

This will certainly cover almost all advertising and targeting cookies, web analytics cookies, and functional services like survey and chat tools that record user identification in cookies.

The GDPR and Consent

Under the existing rules of the ePD, cookies that are not strictly necessary will require consent, and the definition of consent and the requirements associated with it changes significantly under the GDPR.

To understand the impact this might have for cookies, it helps to look at **Recital 32**:

¹¹ Explanatory Memorandum of the draft e-Privacy Regulation proposed by the EU Commission (available at <https://ec.europa.eu/digital-single-market/en/proposal-eprivacy-regulation>)

Consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement. This could include ticking a box when visiting an internet website, choosing technical settings for information society services or another statement or conduct which clearly indicates in this context the data subject's acceptance of the proposed processing of his or her personal data. Silence, pre-ticked boxes or inactivity should not therefore constitute consent. Consent should cover all processing activities carried out for the same purpose or purposes. When the processing has multiple purposes, consent should be given for all of them. If the data subject's consent is to be given following a request by electronic means, the request must be clear, concise and not unnecessarily disruptive to the use of the service for which it is provided.

There is also a key condition for consent in **Article 7(3)**:

The data subject shall have the right to withdraw his or her consent at any time. It shall be as easy to withdraw as to give consent.

The ePD, by contrast, formulated its definition of consent from the old Data Protection Directive, which was much less prescriptive and open to interpretation. For example, earlier drafts of the ePD used the phrase “prior consent,” but the “prior” was later dropped.

The lack of that adjective is what, in many ways, has led to the widely different interpretations of the cookie law that we see today, as noted below. The GDPR is, by contrast, much more specific. A model for cookie consent based on its requirements would suggest many design patterns used in current cookie consent mechanisms must be altered.

Approaches to consent

The proposed e-Privacy Regulation aims at reforming the current e-Privacy Directive to align it with the changes introduced by the GDPR. Consent in the context of electronic communications will now need to meet the conditions of the GDPR (including the requirement that it be informed, specific, freely given, and unambiguous), which will have the following implications:

- **The implied consent approach used by many sites is no longer valid.** Simply visiting a site for the first time would not qualify as affirmative action, which means that loading cookies immediately on the first landing page, would not be acceptable.
- **Advice to adjust browser settings will not be enough.** The GDPR says it must be as easy to withdraw consent as give it. Telling people to block cookies if they don't consent would not meet this criterion. It is difficult and ineffective against non cookie-based tracking, and doesn't provide enough granularity of choice.
- **“By using this site, you accept cookies” statements will not be compliant.** If there is no genuine and free choice, then there is no valid consent. The GDPR also says people who do not consent cannot suffer detriment, which means sites must provide some service to those who do not accept those terms.

- **Sites will need an always-available opt-out.** Even after getting valid consent, there must be a route for people to change their mind, thus fulfilling the requirement that withdrawing consent must be as easy as giving it. If accepting cookies is as easy as clicking a link on a landing page, then withdrawal of consent must be just as simple.
- **Soft opt-in is likely the best consent model.** Website owners should give visitors an opportunity to act before cookies are set on a first visit to a site. Once fair notice is given, continuing to browse can, in most circumstances, be valid consent via affirmative action, but website owners should still consider implementing the persistent opt-out option. This may not be sufficient for sites that contain health-related content, or other sites where the browsing history may reveal sensitive personal data about the visitor. Situations like these could require explicit consent – a much larger hurdle.
- **Sites may need a response to Do Not Track browser requests.** A DNT:1 signal is a valid browser setting that communicates a visitor preference. It can also be interpreted by regulators as a visitor’s right to object to profiling.
- **Consent will need to be specific to different cookie purposes.** Sites that use different types of cookies with different processing purposes will need valid consent mechanisms for each purpose. This means granular levels of control, with separate consents for tracking and analytics cookies, for example.

The Draft e-Privacy Regulation

When the EU Commission launched the public consultation on the ePrivacy Directive, their goals were:

- Ensuring consistency between the ePrivacy rules and the future General Data Protection Regulation
- Updating the scope of the ePrivacy Directive in light of the new market and technological reality
- Enhancing security and confidentiality of communications
- Addressing inconsistent enforcement and fragmentation

A summary report of the responses to the consultation is currently available online¹².

The report shows that seems to be a clear divide between industry opinion and that of citizens and public authorities. While the latter are in favor of stronger rules around tracking technologies stored on users terminal equipment, the former are highly concerned that the current basis for processing such tracking technologies under the draft Regulation are not allowed with those of the GDPR, particularly industry stakeholders are strongly pushing for the addition of “legitimate interest” in the e-Privacy Regulation.

It is also important to understand that the e-Privacy Regulation is *lex specialis*, whereas GDPR is *lex generalis*. This means that when the two regulations cover the same situation (when electronic communications also qualify as personal data), the e-Privacy Regulation will apply (and not the GDPR). As explained in recital 2(a) of the current draft¹³ of the e-Privacy Regulation:

¹² <https://ec.europa.eu/digital-single-market/en/news/summary-report-public-consultation-evaluation-and-review-eprivacy-directive>

¹³ https://iapp.org/media/pdf/resource_center/ePrivReg-council-draft-12-5.pdf

Processing of electronic communications data by providers of electronic communications services should only be permitted in accordance with this Regulation. If no specific rules are established in this Regulation, Regulation (EU) 2016/679 should apply to any processing of electronic communications data that qualify as personal data.

Negotiations on the draft text have been fairly difficult so far, and many believe it is very unlikely the e-Privacy Regulation will be passed by 25 May 2018, which prolongs both uncertainty and risk for businesses needing to implement solutions.

Cookies in the Consultation

Europeans called for stronger privacy protection online, including simpler rules on cookies. Users must be in control of any privacy-sensitive information stored on their devices, without having to click on a banner asking for their consent on cookies each time they visit a website. Browser settings will offer an easy way to allow or refuse cookies. The proposal clarifies that no consent is needed for non-privacy intrusive cookies improving internet experience (e.g. to remember shopping cart history). Cookies set by a visited website counting the number of visitors to that website will no longer require consent.¹⁴

Significant Opinions

European Data Protection Supervisor (EDPS)

The EDPS is the Data Protection Authority for the EU institutions, and will also be a member of the European Data Protection Board under the GDPR.

The position of the EDPS is that the provisions of the ePrivacy Directive should be modernized and strengthened, and that there is a need to “complement and particularise” the GDPR to clarify the relationship between the two instruments. It also points out that elements of ePD are not covered by GDPR, and therefore those elements need to be maintained.

EDPS points out that for legal certainty the core principles of confidentiality of communications found in the EU Charter of Fundamental Rights need a secondary legislation setting out both specific legal requirements and clarifying the relationship with the GDPR. Where the GDPR might allow for several legal grounds for processing of personal data, ePrivacy rules can narrow these options for more specific circumstances – the cookie rules are given as a specific example of this.

The EDPS favors the creation of a new Regulation on the basis that it would be consistent with the approach of the GDPR, enable harmonization of both protections and compliance efforts – with potential cost saving implications – as well as enable further reliance on the one-stop-shop principle in the GDPR.

In stressing that privacy of communications should not be dependent on the content and purpose of the communication, nor the technology used to convey it, the EDPS highlights the differences between privacy and data protection.

¹⁴ e-Privacy fact sheet available at http://europa.eu/rapid/press-release_IP-17-16_en.htm

Confidentiality of communications, both in transit and at rest, should be the key objective of a replacement instrument, as well as creating a level playing field between traditional communications providers (e.g. telecommunications companies) and OTT services. It also believes that separation of content and metadata in communications are increasingly false, especially in Internet services, and therefore protection for the privacy of both types of data are necessary.

With respect to Article 5(3), EDPS says that the definition and interpretation of consent must be consistent with GDPR, and that users should be given “real control” over the use of cookies. Existing consent mechanisms come under attack on the basis that such choice is often non-existent, and only allowing access to content that’s subject to consent to the use of cookies is not seen as consistent with genuine consent.

Recommendations of a partial ban on “cookie walls” are in place so that denial of access to content cannot be made based on an absence of consent. It must be made clearer the situations where choice would not be considered freely given, focusing on situations where the privacy impact is highest, or where there is least amount of freedom of choice, thus impacting both cookie consent and ad-blocking detection.

A recommendation is also in place to build on Recital 66 of the current ePrivacy Directive. This would encourage or require the development of controls in the browser or operating systems that enable the clear expression of consent or its absence with privacy-friendly default settings, and oblige that accepted technical or policy compliance standards be followed by all parties.

This would encompass, for example, a requirement that DNT browser settings must be respected by all parties. A further recommendation for consent exemption for first party analytics is also in place, provided they are purely for aggregated statistical purposes. This would also be subject to an option to opt-out from such collection.

Article 29 Working Party (WP29)

The WP29 is a body made up of representatives of each of the national Data Protection authorities, and will be replaced by the European Data Protection Board under the GDPR. The group regularly publishes opinions and recommendations, which, although are not legally binding, are authoritative and influential with EU legislators.

The position of the WP29 is similar to that of the EDPS – it states that a replacement is needed to ensure the confidentiality of communications as enshrined in Article 7 of the Charter of Fundamental Rights. It points out that the new instrument must “supplement and complement” the obligations under GDPR.

Article 95 of the GDPR, along with Recital 173, states that GDPR should not apply where specific obligations for ePrivacy also exist.

They explicitly state that ePrivacy rules which specify consent as the legal ground for processing prevail over other grounds available in the GDPR, such as legitimate interests.

Their recommendation is that a replacement instrument for the ePD should keep the substance of existing provisions, but also make them “more effective and workable in practice,” by making more precisely defined rules and conditions. Where they differ from the EDPS is in the belief that if the requirements are clear and unambiguous, the needs could be met by either a Regulation or a Directive.

There is agreement, however, that the rules should be extended to OTT services, especially Internet-based communications that are functionally equivalent to traditional telecommunication services.

With respect to consent rules for cookies, WP29 recommends that the wording needs updating to be more technologically neutral and capture a broader range of techniques for what they label as “passive tracking.” This would also include scenarios where signals and data that are necessary for technical transmission of communications are also used for alternative purposes, with specific mention of marketing.

They also recommend more exceptions to the need for prior consent that are aligned with the risk-based approach of the GDPR where there is little impact on privacy.

Much like the EDPS, first party analytics are given as an example of this, if there is both information about them in the privacy policy, and a user-friendly opt-out mechanism.

They also recommend extending the exception for strictly necessary technical purposes to include protection of network or service security, which would include the ability to monitor demand and proactively detect and defend against intrusion.

There is also a recommendation that the need for consent is removed if the data is “immediately and irreversibly anonymized” on the device or network end points.

With respect to existing consent mechanisms used by websites for cookies, the WP29 takes a similar view to the EDPS and agrees that consent is often forced and not genuine.

They even suggest a few circumstances where this should be specifically prohibited, and users should be given the choice to not provide consent and still use the service:

- Services that may reveal an interest in special categories of data;
- Tracking by unspecified parties for unspecified purposes (esp. automated/bid driven advertising);
- Government funded services;
- All circumstances that might lead to consent being invalid under GDPR;
- Where consent for multiple purposes is bundled rather than granular.

They also recommend encouraging controls and/or consent mechanisms that do not rely on individual website operators, but are built into user agents and operating systems.

What are the changes for cookies brought by the draft e-Privacy Regulation?

Under the current Directive, the use of tracking tools and means to access data stored in users' terminal equipment, such as cookies, is allowed with the informed consent of the interested user. Studies have confirmed that the cookies rules, as introduced by the 2009 revision of the ePD, fail to achieve their goal (to enable users to make a real choice and give informed consent), causing, to the contrary, the irritation of users called to repeatedly consent to the use of cookies and faced with 'cookies walls'.¹⁵

¹⁵ [http://www.europarl.europa.eu/RegData/etudes/BRIE/2017/608661/EPRS_BRI\(2017\)608661_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/BRIE/2017/608661/EPRS_BRI(2017)608661_EN.pdf)

Higher Exposure for Non-EU Organizations

As with the GDPR, the new ePrivacy Regulation will have significant extra territorial effects, and will require websites around the world to respect the rights of EU-based visitors. The material and territorial scope of the e-Privacy rules, in light of the new market and technological reality, covers a wider range of services entailing data processing. It applies to the provision of e-communications services to end-users in the Union, irrespective of whether the end-user is required to pay for the service. Providers outside the EU have to appoint a representative in the EU. The proposal applies not only to traditional telecom providers, but also to other market- players (e.g. information society service providers) providing internet-based services, such as VoIP, instant messaging applications and web-based emails (OTTs), with the aim of ensuring a level playing field for companies. It applies to e-communications data processing carried out in connection with the provision and use of e-communications services and to information related to the terminal equipment of end-users. Issues related to the scope of the new regulation, as well as its definitions and exceptions, are currently under discussion.¹⁶

New rules on tracking tools (including cookies)

The collection of information from the end-user's device is allowed only under specific conditions, e.g., for the sole purpose of carrying out the transmission of an electronic communication, or with the end-user's consent, or if it is needed to provide a service requested by the end-user (Article 8.1). The collection of data emitted by terminal equipment, e.g., via WIFI, to enable connection to another device or to a network (Article 8.2) is allowed for the purpose of, and the time necessary for, establishing a connection, or if a clear and prominent informative notice is displayed (according to GDPR Article 13). The latter seems to suggest that user device location tracking is allowed without consent.¹⁷

Privacy settings

In line with the GDPR, when provided, consent must be freely given and unambiguous, but can be expressed by a clear affirmative action. To this end, the new rules provide for the possibility that the consent is given at the level of browser settings, when technically possible and feasible (Article 9), to avoid the consent fatigue caused by current pop-up banners. Article 10 refers to options for privacy settings that browsers should offer to enable users to prevent third parties from tracking online data related to their terminal.¹⁸

Prior (Opt In) Consent

Consent under the old Directive was less clearly defined. It was interpreted differently in each EU country, and many governments allowed an implied consent or opt-out model. The new Regulation explicitly states that the definition of consent will mimic the GDPR, thus shifting the requirements to opt-in only.

This is perhaps the single most significant variance from the old law, and will have widespread implications. The vast majority of websites will need to make changes, some of which will be difficult to apply, thus potentially resulting in future negotiations to improve ease-of-implementation.

Mirroring the GDPR's stance on consent, the new ePrivacy Regulation will require websites to demonstrate that a visitor's consent was obtained, and that their consent can be withdrawn at any time.

An Exemption for Web Analytics

The Directive's old exemptions from the consent rule for "strictly necessary" cookies remain intact, but are now extended to include cookies that are used for web analytics.

¹⁶ [http://www.europarl.europa.eu/RegData/etudes/BRIE/2017/608661/EPRS_BRI\(2017\)608661_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/BRIE/2017/608661/EPRS_BRI(2017)608661_EN.pdf)

¹⁷ [http://www.europarl.europa.eu/RegData/etudes/BRIE/2017/608661/EPRS_BRI\(2017\)608661_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/BRIE/2017/608661/EPRS_BRI(2017)608661_EN.pdf)

¹⁸ [http://www.europarl.europa.eu/RegData/etudes/BRIE/2017/608661/EPRS_BRI\(2017\)608661_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/BRIE/2017/608661/EPRS_BRI(2017)608661_EN.pdf)

This may be a welcome change, as the potential loss of such data was of deep concern to website owners under the old regime. This is slightly qualified in that it only applies to situations where the processing is “carried out by the provider.” It remains to be seen whether popular services like Google Analytics would fit into that exemption. This point will likely require additional clarification moving forward.

Increased Responsibility for Web Browsers

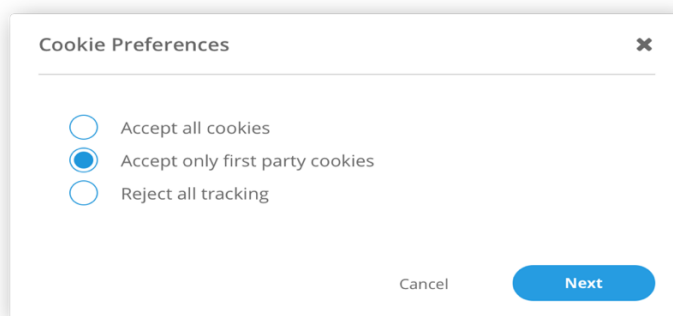
Web browsers are now highly encouraged to take a more active role in mediating consent to avoid the need for overly intrusive pop-ups, but this will rely on some significant changes to the way most browsers currently work.

It remains to be seen whether they will be willing and able to take on such responsibilities, but it seems likely that Do Not Track browser settings will become far more important moving forward.

A new requirement for devices and software to be built on Privacy by Design principles, including privacy as the default setting, was clearly intended to push technology companies toward making big changes, but because Privacy by Design takes a lot of time and effort, it’s unlikely that technology companies will be able to fully comply within the allotted timeline for enforcement.

Under the new rules, end-users should be offered, at the browser level, a set of privacy setting options, ranging from higher (for example, ‘never accept cookies’) to lower (for example, ‘always accept cookies’) and intermediate (for example, ‘reject third party cookies’ or ‘only accept first party cookies’). Such privacy settings should be presented in an easily visible and intelligible manner.

Example:



GDPR-Level Fines

Another area where the ePrivacy Regulation has harmonized with the GDPR is in the enforcement actions and remedies for non-compliance, including provisions for fines of up to €20M, or 4% of a company’s global revenues.

Additionally, the supervisory authorities (data protection authorities) which are responsible for GDPR enforcement will now also be responsible for the enforcement of the e-Privacy Regulation.

Impact on Third Parties

The revised rules are particularly aimed at what the legislators call the “surreptitious monitoring” of online behavior. They call for all third-party storage and processing to be blocked by default. Given the way modern websites are built, often with many tags and code elements served up by third party services, this would have wide-reaching implications, even where privacy is not a significant issue.

It will severely limit the use of third party cookies and tracking that are generally relied upon for monetization of online services — negotiations and lobbying from the online advertising industry on this issue are highly anticipated.

Conflicts and Uncertainties for Site Owners

There are several areas where the current ePD and GDPR are inconsistent, and therefore create complexity for site owners. In theory, the GDPR supersedes national laws on cookies, but it only applies to the subset of cookies that process personal data, so other cookies would still be covered by the ePrivacy Directive. The ePD's definition of consent is drawn from the old Data Protection Directive, but because this was annulled by GDPR, there has been some confusion around the new definition of consent.

The new ePrivacy Regulation will mean that the cost of getting cookie compliance wrong in the future will be much more significant than it is today. It seems inevitable that even with a solid cookie solution in place, website owners will need to make significant changes to ensure continued compliance with the new rules. Companies will also need to pay closer attention to ongoing monitoring of their sites in the future, making sure that they remain compliant with every change they introduce.

Part 2: Operationalizing cookie requirements and best practices


Tips from the EU Commission for lawful cookie use¹⁹

1. Ask yourself whether the use of cookies is essential for a given functionality, and if there is no other, non-intrusive alternative.
2. If you think a cookie is essential, ask yourself how intrusive it is: what data does each cookie hold? Is it linked to other information held about the user? Is its lifespan appropriate to its purpose? What type of cookie is it? Is it a first or a third-party setting the cookie? Who controls the data?
3. Evaluate for each cookie if informed consent is required or not:
 - first-party session cookies DO NOT require informed consent.
 - first-party persistent cookies DO require informed consent. Use only when strictly necessary. The expiry period must not exceed one year.
 - all third-party session and persistent cookies require informed consent. These cookies should not be used on EUROPA sites, as the data collected may be transferred beyond the EU's legal jurisdiction.
4. Before storing cookies, gain consent from the users (if required) by implementing the [Cookie Consent Kit](#) in all the pages of any website using cookies that require informed consent.

Cookie notice/policy

Inform users about the use of cookies in plain, jargon-free language in a dedicated "cookie notice" page linked from the service toolbar of the [standard templates](#). This page should explain:

- why cookies are being used, (to remember users' actions, identify users, collect traffic information, etc.)
- if the cookies are essential for the website or a given functionality to work or if they aim to enhance the performance of the website
- the types of cookies used (e.g. session or permanent, first or third-party)
- who controls/accesses the cookie-related information (website or third-party)
- that the cookie will not be used for any purpose other than the one stated
- how users can withdraw consent.

The EU Commission provides in all EU languages a [standard template to create your own cookie notice page](#)  (241 kB). If a site does not use any cookies, the dedicated "cookie notice" page should use the template and just mention this.

¹⁹ http://ec.europa.eu/ipg/basics/legal/cookies/index_en.htm

Cookie Compliance tools available

EU Commission Cookie Consent Kit²⁰

The cookie consent solution is a JavaScript-based kit that, after some site-specific configuration, will automatically add a header banner to the page. This header banner will disappear once the user has accepted or refused the cookies used on the site.

This solution provides the following functionalities:

- JavaScript to automatically display the header banner in 24 languages
- a wizard to declare your cookies and the link to your cookies notice page
- a JavaScript API with methods and functions that help to prevent prior storage of cookies
- a corporate-consent cookie to remember the choice of the user across websites
- a template for the cookie notice page.

This is a central service: you have to include the JavaScript file on your website and add a one-site-specific configuration file listing the cookies you are using. You will also have to add a short HTML parameter to every element in your site that sets a cookie.

CNIL How to Guide for websites, cookies and other tracking technologies

The CNIL offers on its website (available in French) a comprehensive guide²¹ to help website publishers, app developers, ad networks, operating systems, social networks and website analytics providers navigate the different cookie requirements. The guide includes a summary of the legal requirements, examples of a lawful cookie banner, solutions for centralized consent management, social buttons (such as the Facebook like button), measuring web trafficking, and advertising.

The CNIL guidance specifies which cookies it considers to be exempt from the consent requirement under French data protection law:

- cookies used for a “shopping basket” on a merchant’s website;
- “Session ID” cookies for the duration of the session (or persistent cookies limited to a few hours in some cases);
- authentication cookies;
- multimedia player session cookies;

²⁰ http://ec.europa.eu/ipg/basics/legal/cookies/index_en.htm

²¹ <https://www.cnil.fr/fr/site-web-cookies-et-autres-traceurs>

- load balancing session cookies; and
- persistent user interface customization cookies.

Some web analytics solutions also may qualify for an exemption from the consent requirement.

In all other cases, the CNIL's Guidance emphasizes that:²²

- web users' consent must be obtained before placing or reading cookies and similar technologies (such as web bugs and fingerprinting technologies), and such consent must be obtained each time these technologies are used for a new purpose;
- the validity of the consent is linked to the quality of the information provided to web users – in particular, web users must be clearly informed of the different purposes for which the cookies and similar technologies will be used; and
- web users' consent is valid only if the users have a real choice between accepting or refusing cookies and similar technologies.

OneTrust Cookie Compliance

OneTrust provides a comprehensive solution to help businesses meet the requirements for cookie consent. Our commitment to ongoing development means that as the legislative requirements change and new rules are imposed, we will ensure we continue to meet our customers' needs. The OneTrust Cookie module allows you to do the following:

Automated Auditing

Cookie compliance starts with having an accurate understanding of what cookies and tracking technologies your sites are using. Only then can you make the proper risk-based decisions, and ensure your visitors are fully informed. Websites and the technologies they are built on are constantly changing — website owners need a service that can keep up.¹⁰ Our auditing solution combines the power of the cloud with the unrivalled knowledge base of Cookiepedia to deliver regular, fully automated reports on your sites, giving you all the information you need to make sure you can both get and remain compliant.

Flexible Notice

We provide website owners with the necessary tools to put a cookie notice on their websites, and with simple deployment and full editorial control over the content and user experience. OneTrust supports a wide range of user journey options and consent models, brand customization, and multi-lingual capabilities, allowing customers to easily tailor notices to their audiences.

Our Software-as-a-Service model means changes can be instantly updated to a live website without waiting for IT deployment cycles, giving the privacy and compliance team the autonomy they need to adapt to the changing regulatory landscape.

Real Consent and Control

²² <https://www.huntonprivacyblog.com/2013/12/18/french-data-protection-authority-issues-guidance-cookie-consent-expiration/>

Giving visitors the ability to consent to or deny cookies is important for true cookie compliance. With a rich mix of methods for responding to visitor choices, including integration with tag management services, OneTrust gives website owners the power to provide granular controls for visitors, respecting their preferences while ensuring the website owner's control of the overall user experience.

Support from a Team of Experts

Adhering to cookie compliance laws is not as simple as it seems. Implementation of a solution often involves the needs, interests, and perspectives of business teams like marketing, legal, privacy, and IT. OneTrust's experienced support team works with all these stakeholders to ensure customers meet their policy and legal commitments.

Part 3: Additional resources

Article 29 Working Party

- Opinion 15/2011 on the definition of consent
http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp187_en.pdf
- Opinion 04/2012 on Cookie Consent Exemption
http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp194_en.pdf

ICO

- Guidance on the rules on use of cookies and similar technologies
https://ico.org.uk/media/for-organisations/documents/1545/cookies_guidance.pdf
- Privacy in Mobile Apps: Guidance for App Developers
<https://ico.org.uk/media/for-organisations/documents/1596/privacy-in-mobile-apps-dp-guidance.pdf>

CNIL

- Websites, cookies and other tracking technologies: How to Guide
<https://www.cnil.fr/fr/site-web-cookies-et-autres-traceurs>

About OneTrust

OneTrust is a global leader in enterprise privacy management software used by more than 1,500 organisations to comply with data privacy regulations across sectors and jurisdictions, including the renowned EU General Data Protection Regulation (GDPR).

OneTrust is among the most widely used global technology solutions to implement a GDPR-based privacy compliance programme. The comprehensive OneTrust platform helps organisations track the full lifecycle of their personal data flows, analyse these data flows against global regulations to understand risks, communicate directly with customers, employees, and vendors to capture consent, handle privacy-related requests, and respond appropriately in the event of an incident.



The multi-lingual software is deployed in an EU cloud or on-premise, and is based on a combination of intelligent scanning, regulator guidance-based questionnaires, and automated workflows used together to automatically generate the record keeping required for an organisation to demonstrate compliance to regulators and auditors.

OneTrust helps organisations implement the requirements of GDPR including Data Protection by Design, Data Protection Impact Assessments (PIA / DPIA), Vendor Management, Incident and Breach Management, Records of Processing (Data Mapping), Consent Management, ePrivacy Cookie Compliance, Data Subject Access, Portability, and Right to Be Forgotten.

Backed by the founders of Manhattan Associates (NASDAQ: MANH) and AirWatch (\$1.54B acq. by VMware), OneTrust is co-headquartered in London, UK and Atlanta, GA with a fast-growing global team of privacy and technology experts surpassing 200 employees.

OneTrust

Global Leader for Privacy Management Software

 <div style="background-color: #4CAF50; color: white; padding: 5px; font-weight: bold; font-size: 0.9em;">Readiness & Accountability Tool</div> <div style="background-color: #f0f0f0; padding: 5px; font-size: 0.8em;"> Article 5: Principles Relating to Processing of Personal Data Article 24: Responsibility of the Controller </div> <div style="background-color: #333; color: white; padding: 5px; font-size: 0.8em;">Centrally document compliance with GDPR</div>	 <div style="background-color: #4CAF50; color: white; padding: 5px; font-weight: bold; font-size: 0.9em;">PIA & DPIA Automation</div> <div style="background-color: #f0f0f0; padding: 5px; font-size: 0.8em;"> Article 25: Data Protection by Design & Default Article 35: DPIA Article 36: Prior Consultation </div> <div style="background-color: #333; color: white; padding: 5px; font-size: 0.8em;">Review new business projects for privacy risks</div>	 <div style="background-color: #4CAF50; color: white; padding: 5px; font-weight: bold; font-size: 0.9em;">Data Mapping Automation</div> <div style="background-color: #f0f0f0; padding: 5px; font-size: 0.8em;"> Article 30: Records of Processing Activities Article 32: Security of Processing </div> <div style="background-color: #333; color: white; padding: 5px; font-size: 0.8em;">Inventory the business context of your data flows</div>	 <div style="background-color: #4CAF50; color: white; padding: 5px; font-weight: bold; font-size: 0.9em;">Website Scanning & Cookie Compliance</div> <div style="background-color: #f0f0f0; padding: 5px; font-size: 0.8em;"> Article 7: Conditions for Consent Article 21: Right to Object ePrivacy Directive / Draft Reg. </div> <div style="background-color: #333; color: white; padding: 5px; font-size: 0.8em;">Update consent notices on your web properties</div>
 <div style="background-color: #4CAF50; color: white; padding: 5px; font-weight: bold; font-size: 0.9em;">Subject Access Request Portal</div> <div style="background-color: #f0f0f0; padding: 5px; font-size: 0.8em;"> Articles 12 - 21: Rights of the Data Subject </div> <div style="background-color: #333; color: white; padding: 5px; font-size: 0.8em;">Portal to handle the full lifecycle of subject requests</div>	 <div style="background-color: #4CAF50; color: white; padding: 5px; font-weight: bold; font-size: 0.9em;">Consent Receipt Management</div> <div style="background-color: #f0f0f0; padding: 5px; font-size: 0.8em;"> Articles 7: Conditions for Consent </div> <div style="background-color: #333; color: white; padding: 5px; font-size: 0.8em;">Maintain evidence of each individual's consent</div>	 <div style="background-color: #4CAF50; color: white; padding: 5px; font-weight: bold; font-size: 0.9em;">Vendor Risk Management</div> <div style="background-color: #f0f0f0; padding: 5px; font-size: 0.8em;"> Articles 28, 24 & 29: Responsibilities of Processor & Controller Article 46: Transfer Subject to Appropriate Safeguards </div> <div style="background-color: #333; color: white; padding: 5px; font-size: 0.8em;">Properly vet any sub-processors for onward transfers</div>	 <div style="background-color: #4CAF50; color: white; padding: 5px; font-weight: bold; font-size: 0.9em;">Incident & Breach Management</div> <div style="background-color: #f0f0f0; padding: 5px; font-size: 0.8em;"> Article 33: Notification to Supervisory Authority Article 34: Notification to Data Subject </div> <div style="background-color: #333; color: white; padding: 5px; font-size: 0.8em;">Collection and notification workflow for incidents</div>