The Future of EU Cookie Compliance: GDPR and the ePrivacy Directive Revision

Current requirements for cookie consent notices on websites are derived from the ePrivacy Directive (ePD), the current version of which came into effect in 2011, although specific requirements for compliance with cookie rules are written into national legislation in each EU Member State.

In the first half of 2016, the EU Commission launched a public consultation on the future of the ePrivacy Directive, driven in part by the introduction of the GDPR, but also prescribed as part of the wider Digital Single Market Strategy, launched in 2012.

It was originally announced that a proposal for replacement legislation would be released towards the end of 2016, but is now expected to be released in early 2017; however, in mid-December 2016, a draft of the new instrument was leaked. A copy of the document can be found on Politico.eu.

What to Expect based on the Leaked Draft

The leaked document states that the replacement law will "particularize and complement" the EU GDPR, which enables it to become a much simpler legal instrument. Many of its original provisions, such as data breach requirements, are now part of the GDPR. It is also further harmonized with the GDPR by relying on many of its key definitions, as well as aligning its enforcement regime, including potential fines.

The draft shows that the new law will maintain its broad focus on communications privacy, and brings over-the-top (OTT) Internet services into its remit for the first time. This document will focus on the key parts that impact cookie compliance.

A Regulation Rather than a Directive

The main impact of the new regulation should be a single set of cookie rules for all EU countries, which will be a significant simplification for many businesses, particularly those operating in multiple markets. This will largely mean that the different consent models used in different countries will disappear, which makes implementation easier, and gives end-users greater clarity and consistency.

Six Month Compliance Timeline

While we can expect there to be a reasonable amount of time for this draft to be lobbied and negotiated, the Commission has proposed a mere six-month lead-in period from the time the law is passed to its eventual enforcement, which indicates their desire to enforce the new ePrivacy Regulation and GDPR congruently. By contrast, the Commission allotted a two-year lead-in period for GDPR, which means a six-month timeline will not give businesses enough time to react.

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.

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.

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.

GDPR-Level Fines

Another area where the ePrivacy Regulations have 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 bodies will now be the same organizations responsible for GDPR, which, under the current rules, has not always been the case.

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.

The Evolution of Cookie Consent Regulations

ePrivacy Directive Overview

The ePrivacy Directive (ePD) was first introduced in 2002, and revised in 2009. It is primarily concerned with the confidentiality of communications, and many of its requirements specifically target telecommunications companies. This includes within its remit, to some extent, the privacy of communications over the Internet.

ePrivacy Directive on Cookies

We've narrowed the focus of this white paper to Article 5(3), which, in short, requires that any "storing or retrieving" of information from an end users' device should 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".) In 2014, Apple "gifted" a free album from U2 to all iTunes users, by initiating an automatic download to iPods and iPhones. While this upset a lot of people for many different reasons, it was the storing of information in the form of a music file without consent that was seen as more of a breach of the ePrivacy Directive.

Web cookies are the most common technology to be directly impacted by the consent rule, so the term is used to cover all such technologies in most discourse on the subject, and, as a result, became widely known as the Cookie Law.

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. 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 a quite narrow.

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.

Application and Enforcement

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/signified, 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) has been in effect since May 2016, though it will be May 2018 before it will be enforced, which means that now is the time to align business practice to its requirements.

As a regulation, the GDPR is both directly applicable and supersedes national laws except where they are explicitly allowed. Though seen as a comprehensive law, the GDPR is in some ways narrower than the ePD because it **only** applies to personal data, but it has much greater reach in that it applies to a broader range of scenarios and conditions under which personal data can be processed, beyond the consent-only approach of the ePD.

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 is 1 recital that is 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.

GDPR on 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:

> *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, reportedly with significant lobbying from the UK government.

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.

- **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 won't 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 don't consent can't suffer detriment, which means sites must provide some service to those who don't 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.

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's been some confusion around the new definition of consent.

Cookies covered by GDPR could potentially rely on a legal basis other than consent, the most obvious of which is legitimate business interests. As consent is the only legal basis under ePD, this sets up a scenario where a cookie that does not involve personal data processing could be subject to more stringent requirements than one that does, e.g. a persistent cookie that stores information about the screen size of the end-user device.

This type of cookie doesn't store enough information to be considered personal data, so GDPR would not apply here, but it's also not likely to be "strictly necessary," as, at most, the website would only need this information for one session. It may be beneficial optimization and performance, but it's not a necessary cookie, therefore, it would require consent, while a cookie containing personal data may not.

Though not a main driver to revise the ePD, this example certainly makes the case for providing additional clarity around anomalies or uncertainties regarding cookie law.

The Making of the New ePrivacy Law

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 online.

This indicates that there are significant differences of opinion about the future of this piece of legislation. More specifically, there seems to be a clear divide between industry opinion and that of citizens and public authorities.

It may be reasonable to expect difficult and protected negotiations over the proposed changes, which could mean that there may not be an agreed upon text before GDPR enforcement begins. This only serves to prolong both uncertainty and risk for businesses needing to implement solutions.

Cookies in the Consultation

Very little of the consultation questionnaire directly addressed the issue of Article 5(3) and its position in future legislation. A direct question was asked about whether it would be considered acceptable if the provision of online services were denied to users if they refuse to give consent for the use of cookies – most citizens and public entities believed this should not be allowed, while a similar industry majority thought it should.

Significant Opinions

When considering what the future scope of the ePrivacy Directive might be, particularly in relation to cookie consent, it's useful to look beyond the consultation responses and take into consideration the published opinions of several influential bodies, including the European Data Protection Supervisor (EDPS), Article 29 Working Party (WP29) and Centre for Information Policy Leadership (CIPL).

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.

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 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.

Centre for Information Policy Leadership (CIPL)

CIPL is a highly respected think tank, associated with leading law firm Hunton & Williams, and funded by its members which include a wide range of global organizations, including major technology, pharmaceutical, and financial businesses.

The position of CIPL is very different from the EDPS and WP29. Although it makes less specific recommendations particularly in relation to consent for cookies, there are several relevant elements in their positioning.

CIPL agrees that there is a need to revise the ePD on the basis that the relationship with the GDPR is unclear and that there are significant overlaps between the two instruments. Where the EDPS and WP29 feel that the more specific rules of ePrivacy should take precedence over GDPR, the CIPL position is the opposite: GDPR should take precedence over a revised ePrivacy instrument.

CIPL agrees with EDPS that there should be a Regulation for the revised instrument.

CIPL's position and recommendations are unclear with respect to cookies and cookie consent. Their position paper only makes broad recommendations that the aspects of the ePD dealing with confidentiality of communications (which includes the cookie rules) should not overlap with other legislation, though the other instruments they mention, apart from the GDPR, do not cover consent for cookies in any exclusive form.

CIPL's response makes the case that the ePD should not contain any obligations with respect to confidentiality of communications, which would include cookie rules, and that it should defer to the GDPR. They also point out their belief that inconsistent national implementations of the cookie rules have made it difficult for international businesses to comply, and give little benefit to individuals, which is also acknowledged by both the EDPS and WP29.

Conclusion

Agreement is widespread that the ePrivacy Directive needs updating, and that its relationship with the GDPR needs clarification. Given the wider move towards harmonization, especially in the wider context of the Digital Single Market, it seems almost inevitable that the revised instrument would be proposed as a Regulation in the way that it has.

The leaked document will be negotiated and lobbied many times over before it meets standards that will satisfy both businesses and consumers; thus, the passage of this new legislation isn't expected to be a smooth transition.

Next Steps for Website Owners

The new ePrivacy legislation 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.

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.

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.

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

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 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.