OneTrust

PRIVACY, SECURITY & GOVERNANCE

THE ULTIMATE COOKIE HANDBOOK FOR PRIVACY PROFESSIONALS

THE ULTIMATE COOKIE HANDBOOK FOR PRIVACY PROFESSIONALS

NOVEMBER 2020

Table of Contents

Table of Contents 4

Part 1: Understanding the Terminology and Requirements 5

Part 2: Operationalizing EU Cookie Requirements and Best Practices 29

Part 3: CCPA Requirements, Rights and Terminology 42

Part 4: OneTrust Solutions 55

Part 5: FAQs 57

NOVEMBER 2020

Part 1: Understanding the Terminology and Requirements

Terminology

Overview of Cookies

When a user visits a website, the website requests the user's browser to store a cookie on the computer or mobile device. A cookie is a small piece of data (text file), generated by a website, that remembers information about users and website usage, such as 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.

For example, websites use cookies to:

- Identify users;
- Remember users' custom preferences (such as language preference); and
- 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; or
    - 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"

However, cookies can also be used by search engines and online advertisers for online behavioral advertising usually enabled by a third-party (not the website publisher) who is usually an ad tech vendor.

Cookies are enabled by the publisher of a website or by third parties.[1] Originally, they were created to enable e-commerce solutions for the web, as the web did not have memory capabilities (e.g. to remember what items have been added to a shopping cart and by whom). Today, cookies are meant to enhance the overall experience of a person visiting a website by tracking a wide range of data such as user preferences, activity, login details, IP addresses, location, etc.

Different Types of Cookies

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

- 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.

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

- First-party cookies which are set by the web server of the visited page and share the same domain; or
- 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.

A commonly accepted classification of cookies according to their purpose includes five different categories:

- Strictly necessary cookies: these are essential cookies enabled for the proper functioning of websites and are used to perform basic functions. Without these cookies a website may not function as intended.
- Performance cookies: they collect information about how visitors use a website – usually aggregated information that does not identify individuals. The information collected is used to provide publishers with statistical information about the site. Typically, analytics cookies are found in this category.
- Functional cookies: these are cookies that are generally there to support site functionality that is visible or advantageous to the user or their experience of the site, they enable websites to remember choices and provide a more personalized experience.
- Targeting cookies (advertising): these cookies are enabled in behavioral advertising contexts. They are usually set by digital advertising businesses for the prime or sole purpose of managing the performance of adverts, displaying adverts, and/or building user profiles. Typically, these cookies would be set by a third-party buying ad space (or impressions) on a website.

There are other 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 again. 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.

Third-Party Cookies

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 device by a website from a domain other than the one you are visiting. The most common third-party cookies are enabled by social media platforms, marketers, advertisers and ad tech companies. Third-party cookies embed a "piece" of their website in a different website, and this allows them to store cookies on your machine, in addition to those stored by the first party. For example, if you visit a news website and the site has 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. This other website can also store a cookie on your device, which is a third-party cookie.

Third party cookies have been used by marketers since the late 90s to track users' online behavior and user experience was personalised by them with individual ads in line with their interests. Usually, third parties buy ad space on websites through a process called Real Time Bidding (RTB) based on the limited information they receive about the potential interests of the website visitors. Usually, ads and content delivered this way are tailored to the interests of website visitors, therefore potentially highly invasive of their privacy, mainly due to the fact that website visitors are largely unaware of this process and the ways their personal data are processed and shared with third parties in order to achieve personalisation.

Real Time Bidding (RTB)

RTB is the process of selling and buying ad space, or impressions, on websites for ad tech vendors to show to website visitors. This

is achieved through a real-time, online auction of ad space in the form of a programmatic instantaneous tender that is triggered when a user visits a website. Once a bid request is triggered an auction starts and the ad space or internet impression goes to the highest bidder, which serves the ad on the page. The bid request usually generates a data set about the user that includes information such as demographics, browsing history, location, and the page being loaded, which will then be used for the advertiser to publish a targeted ad on the impression bought. This process takes no longer than the time it takes a webpage to load when a user visits a website.

There are three main parties involved with the RTB process:

- Publishers: they usually are controllers of personal data as defined in the GDPR and are the ones that initiate the auction by sending bid requests every time a user loads a webpage.
- Ad tech vendors: parties bidding for internet impressions (ad space) as a site loads onto a user's equipment. The request for a bid is passed from the publisher (of the website the user is loading) to an ad exchange platform.
- Ad exchange platforms: give advertisers access to information used to determine the value of a specific impression and, at a larger scale tailor specific marketing campaigns to specific groups of users.

Consent Management Providers (CMPs)

Digital consent management is a process whereby website publishers meet privacy requirements, through the use of an interface that can developed in-house, or more commonly by a third party. CMPs help website operators and publishers with their data processing obligations, including ePrivacy and GDPR obligations, as well as CCPA requirements in California. Digital consent management usually takes the form of layered information

presented to users, and a preference mechanism that provides granular cookie choice to users. CMPs are providers that enable website publishers to automate their consent management processes, they typically are data processors of website publishers and must comply with GDPR processor obligations. The term CMP was coined in the context of the IAB Transparency and Consent Framework.

Transparency and Consent Framework (TCF)

The TCF is an industry framework delivered by the Interactive Advertising Bureau (IAB) Europe designed to help entities in the digital advertising ecosystem achieve transparency and downstream user choice to third parties. Publishers, advertisers and CMPs can voluntarily apply to adhere to the technical specifications and policies of the framework. The framework is dynamic and is updated according to the circumstances, currently we expect v2.0 of the framework to be fully implemented 15 August 2020. Each party involved in the TCF has its own responsibilities for ensuring the proper implementation of the technical specifications, support of obligatory features and compliance with the policies.

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

Device and browser fingerprinting are common tracking techniques that are more subtle than cookies. Device fingerprinting allows the identification of devices by collecting information stored in applications that are locally installed. The information stored by local applications may include unique identifiers, such as a MAC address and serial numbers, making it possible to identify users. The technology can identify a user even when cookies are turned off or have been deleted.

Browser fingerprinting consists in collecting large amounts of diverse and stable information that is unique to each family of web browsers. In addition, by using this technique “fingerprinters” can retrieve information about browser plug-ins and extensions, browsing history and hardware properties.

Although this handbook focuses on cookies, the ePrivacy Directive and proposed draft ePrivacy 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). At the same time, the draft ePrivacy Regulation (addressed in page 24 of this handbook) would apply to both the use of processing and storage capabilities of users’ terminal equipment and the collection of information from the same terminal equipment, covering types of tracking technologies that go beyond the concept of cookie.

Requirements for EU Regulations and Frameworks

The ePrivacy Directive

The ePrivacy Directive is primarily concerned with the confidentiality of electronic communications in publicly available communications networks, and many of its requirements cover publicly available telecommunications services.

Current requirements for cookies in Europe are derived from the ePrivacy Directive, the current version of which came into effect in 2011. Unlike regulations, Directives are not directly applicable in Member States; they must be transposed into domestic legislation.

The ePrivacy Directive is primarily concerned with the confidentiality of electronic communications in publicly available communications networks, and many of its requirements covers publicly available telecommunications services's. Industry frameworks, such as the TCF reflect this obligation in their policy. For example, the TCF lists several purposes and the available lawful processing grounds available for each purpose. The first purpose in the list reflects the obligation contained in Article 5(3) of the ePrivacy Directive, namely, to obtain consent for the use of tracking technologies in general, regardless of the nature of the data that they process.

Consent: The Only Legal Basis Available for Cookies

Article 5(3) of the ePrivacy Directive, requires, in short, that any "storing or retrieving" (writing or reading) of information from an end user' 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.

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 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).

Cookies 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 for the provider of an information society service explicitly required by the user to provide that service.

Cookies clearly exempt from consent according to the EU advisory body on data protection, the Article 29 Working Party, now European Data Protection Board ('EDPB'), 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 customization 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. This strict consent requirement contrasts with comprehensive data protection and privacy laws, such as the General Data Protection Regulation ('GDPR'), which allows for additional legal grounds for processing (like legitimate interest, or necessity for the performance of a contract).

The Directive Created a Fragmented Landscape in the EU

One of the key difficulties with the ePrivacy Directive 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 created 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. 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 publishers and confusing for end-users, who find themselves presented with a broad range of choices on 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 GDPR entered into force on 25 May 2018. As regulations are directly applicable in each Member State, the goal of the GDPR was to harmonize the data protection framework across the European Union.

While the ePrivacy Directive ensures the protection of fundamental rights and freedoms, it covers the respect for private life and confidentiality of communications in the electronic communications sector. On the other hand, the GDPR covers all matters concerning the processing of personal data not specifically addressed in the ePrivacy Directive or future ePrivacy Regulation.

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, 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 ePrivacy Directive, 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 of the GDPR:

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) of the GDPR:

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 definition of consent as contained in the GDPR is, therefore, specific. The adaptation of consent-collecting mechanisms in light of the definition of consent under the GDPR is something organizations must bear in mind, especially since the topic of cookies has been a major focal point for European regulators during 2019. In fact, supervisory authorities intervened from both a policy and enforcement perspective, issuing guidance and recommendations directed at data controllers and enforcing existing provisions. The different positions of the main European data protection authorities are examined in further detail in Part 2 of the handbook.

Approaches to Consent

The proposed ePrivacy Regulation aims at replacing the current ePrivacy Directive to align the legislation 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 necessity to be informed, about specific purposes, freely given and unambiguous consent), which will have the following implications:

- The implied consent approach 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 is not enough. The GDPR says it must be as easy to withdraw consent as to give it. Telling people to block cookies if they don't consent would not meet this criterion, since it would be difficult and ineffective in relation to non-cookie-based tracking and would not provide enough granularity of choice.
- 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 because of their choice, which means that sites must provide some service to users who do not accept those terms.
- Sites must implement an always-available opt-out mechanism. 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.
- Website publishers should give visitors an opportunity to act before cookies are set on the first visit to the site. Once fair notice is given, continuing to browse won't be, in most

circumstances, a valid consent obtained via an affirmative action. Certain exceptions to this rule are provided by the Spanish data protection authority, as explained in Part 2 of the handbook. In any case, website publishers should still implement the persistent opt-out option. Specific precautions will also have to be adopted for sites that contain health-related content, or other sites where the browsing history may reveal sensitive personal data of the visitor.

- Consent needs 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 ePrivacy Regulation

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

- Ensuring consistency between the ePrivacy rules and the GDPR;
- Updating the scope of the ePrivacy Directive in light of the new market and technological reality;
- Enhancing security and confidentiality of communications; and
- Addressing inconsistent enforcement and fragmentation.

It is also important to understand that the ePrivacy Regulation would be lex specialis, whereas the GDPR is lex generalis. This means that when the two regulations cover the same situation (when electronic communications also qualify as personal data), the ePrivacy Regulation will apply instead of the GDPR. As

explained in Recital 2(a) of the current draft12 of the ePrivacy Regulation:

This Regulation protects in addition the respect for private life and communications. The provisions of this Regulation particularise and complement the general rules on the protection of personal data laid down in Regulation (EU) 2016/679. This Regulation therefore does not lower the level of protection enjoyed by natural persons under Regulation (EU) 2016/679. The provisions particularise Regulation (EU) 2016/679 as regards personal data by translating its principles into specific rules. If no specific rules are established in this Regulation, Regulation (EU) 2016/679 should apply to any processing of data that qualify as personal data. Processing of electronic communications data by providers of electronic communications services and networks should only be permitted in accordance with this Regulation.

Negotiations on the draft text have been difficult so far, and there is still uncertainty on the likeliness of approval, which prolongs both uncertainty and risks for businesses needing to implement compliant solutions.

What Are the Changes for Cookies Brought By the ePrivacy Regulation Draft?

Under the ePrivacy 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. However, the practice confirmed that the cookies rules, as introduced by the 2009 revision of the ePrivacy Directive, struggle

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'.

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 Regulation, considering 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. In addition, providers outside the EU must 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, 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.

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, with the end-user's consent, if it is needed to provide a service

requested by the end-user, or for audience measuring purposes (Article 8(1) of the draft ePrivacy Regulation). 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) of the draft ePrivacy Regulation) is allowed:

- For the purpose of, and the time necessary for, establishing a connection.
- If the user has given his/her consent.
- If it is necessary for the purpose of statistical counting, when the data is made anonymous or erased as soon as it is no longer needed.
- If it is necessary for providing a service requested by the user.

In any case, the service provider must provide a clear and prominent informative notice (according to Article 13 of the GDPR) and adopt appropriate technical and organizational measures.

Privacy Settings

In line with the GDPR, when provided, consent must be freely given and unambiguous, as well as 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 4a of the draft ePrivacy Regulation), in order to avoid the consent fatigue caused by current pop-up banners.

Prior (Opt-In) Consent

The draft ePrivacy Regulation explicitly states that the definition of consent will mimic the GDPR, thus shifting the requirements to opt-in only.

Mirroring the GDPR's stance on consent, the draft 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 ePrivacy 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 publishers under the old regime. The new provision applies to situations where the processing is carried out by the provider or by a third party on his behalf, if the conditions laid down in Article 28 of the GDPR, or where applicable, Article 26 of the GDPR (i.e. joint controllership), are met. It remains to be seen whether popular services like Google Analytics would fit into that exemption, considering the sometimes-divergent position adopted by European regulators.

Increased Responsibility for Web Browsers

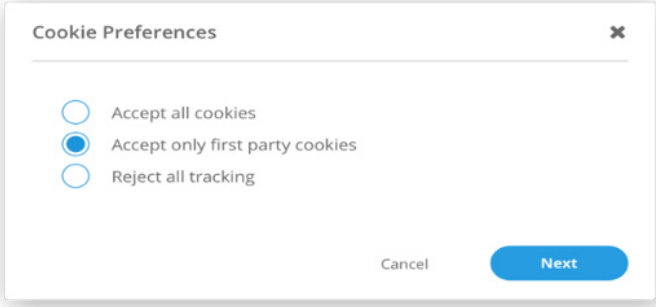
Web browsers are now highly encouraged to take a more active role in mediating consent to avoid the need for overly intrusive pop-ups, but this will rely on some significant changes to the way most browsers currently work.

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.

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:



Latest Developments on the ePrivacy Regulation

The German Presidency of the Council of the European Union released, on 6 July 2020, a new discussion paper on the proposed ePrivacy Regulation, outlining that it would like to reach a general approach and/or a mandate to start negotiations with the European Parliament.

Specifically, the Presidency stressed the fact that an agreement on the core provisions of the proposal, namely the rules for the protection of end users' terminal equipment information is a precondition. In fact, and in relation to cookies and similar technologies the progress report, the progress report provides that:

- Should the proposals to permit access to terminal devices for the sole purpose of a legitimate interest (as outlined above), subject to specific conditions and safeguards, be supported, the Presidency would like to discuss how the security of the respective equipment can be ensured under these conditions.
- Should the last proposal of the Finnish Presidency be supported, the Presidency would like to ask the Member States whether they see a need to further discuss the provision related to requirements for access to terminal equipment in connection with IoT devices and with regard to the effective protection of end users' privacy.

As a consequence, in the most recent compromise draft, published on 4 November 2020, the Presidency deleted any reference to the provisions on the use of processing and storage capabilities of terminal equipment and the collection of information from end-users' terminal equipment when necessary for the purpose of legitimate interests.

In addition, the last compromise proposal has introduced a stricter wording aimed to define clearly the conditions when the use of terminal equipment is necessary for providing a service specifically requested by the end-user. In this regard, the draft provides that the setting of cookies, in order to be allowed, must be 'strictly technically necessary for providing an information society service specifically requested by the end-user'.

The compromise proposal has also re-introduced the possibility of setting cookies and similar tracking technologies when the same is necessary for:

- Security Purposes: To maintain or restore the security of end users' information society services or terminal equipment, prevent fraud or detect technical faults for the duration

necessary for that purpose.

- Software Updates That Do the Following:
    1. Is necessary for security reasons and does not change the user's privacy settings.
    2. Informs the end user in advance of the update installation.
    3. Gives the end user the possibility to postpone or turn off the automatic installation of the update.

Moreover, the EDPB issued, on 19 November 2020, a statement on the future of the ePrivacy Regulation, welcoming the idea of adopting the same as soon as possible. However, and in relation to the regulation of cookies, the EDPB also stressed the lost opportunity to provide guidance on the practice of cookie walls within the text of the regulation itself.

However, the German Presidency of the Council, after the Member States meeting within the Council's Working Party on Telecommunications and Information Society, published, on 20 November 2020, a new progress report on the draft ePrivacy Regulation. In particular, the report recalls the amendments proposed by the German Presidency in the last compromise proposal, specifying though that Member States had mixed reaction to the same, and that, even if they reached a broad consensus around the deletion of any reference to legitimate interests as a legal basis for cookies, they also expressed the view that the former Finnish Presidency proposal could be considered as the starting point for future negotiations. In conclusion, the German Presidency notes that it is clear from the Member States' reactions that further work is needed on the file, and that it is committed to working closely with the forthcoming Portuguese Presidency to facilitate further discussions and to ensure smooth progress on the proposal.

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 ePrivacy 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.

Part 2: Operationalizing EU Cookie Requirements and Best Practices

Tips from the EU Commission for Lawful Cookie Use

- Ask yourself whether the use of cookies is essential for a given functionality, and if there is no other, non-intrusive alternative.

- 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?
- 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.
- 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 publisher 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 (241kB). If a site does not use any cookies, the dedicated "cookie notice" page should use the template and just mention this.

Recommendations from EU Institutions and European Data Protection Authorities

At the EU-level, the most recent opinions issued by the European Data Protection Supervisor ('EDPS') and the Article 29 Working Party ('WP29') on the reform process of the ePrivacy Directive are from 2017 and 2016, respectively. However, they are still able to give an idea of the EU regulators' vision in relation to the ePrivacy rules evolution process.

EDPS – Opinion No. 6/2017 on the ePrivacy Regulation

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.

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

With respect to Article 5(3) of the ePrivacy Directive, the EDPS believes that the definition and interpretation of consent must

be consistent with the GDPR, and that users should be given "real control" over the use of cookies. The EDPS also stresses the fact that only allowing access to content that's subject to consent to the use of cookies is not consistent with genuine consent.

The EDPS also think that it must be clarified 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 further recommendation for consent exemption for first party analytics is also in place, provided they are purely for aggregated statistical purposes.

WP29 - Opinion No. 3/2016 on the evaluation and review of the ePrivacy Directive

The position of the WP29 is similar to the one of the EDPS. The WP29 thinks that a replacement instrument for the ePrivacy Directive 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.

With respect to consent rules for cookies, the 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."

They also recommend more exceptions to the need for prior consent, in light of the risk-based approach of the GDPR, where there is little impact on privacy. 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.

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.

EDPB, CJEU and National Data Protection Authorities

More recently, the implementation of cookies' requirements has been addressed by the European Data Protection Bouar ('EDPB'), the Court of Justice of the European Union ('CJEU') and national data protection authorities. Organizations can now access a various range of practical recommendations in order to enable a compliant approach to cookies.

EDPB

The EDPB adopted, on 4 May 2020, its Guidelines 05/2020 on Consent under Regulation 2016/679. In particular, the Guidelines represent a slightly updated version of the Article 29 Working Party's Guidelines on Consent under Regulation 2016/679, which were endorsed by the EDPB in its first plenary meeting. The updated Guidelines, which should from now on replace any reference to the WP29 Guidelines, provide clarification on the following cookies-related points:

- The validity of consent as provided by data subjects when interacting with 'cookie walls'.
- The action of scrolling or swiping through a webpage, or similar user activity, as a clear and affirmative action of consent.

Conditionality as an element of a freely given consent

Key recommendations:

- Service providers cannot prevent data subjects from accessing a service on the basis that they do not consent.
- 'Cookie walls' are not permitted: access to services and functionalities must not be made conditional on the consent

> of users to the placement of cookies or similar technologies on their terminal equipment.

When data controllers offer a choice between their service, that includes consenting to the use of personal data for additional purposes, and an equivalent service offered by a different controller, consent cannot be considered as freely given. In fact, in such a case, the freedom of providing consent would be made dependent on what other market players do and whether data subjects would find the other data controller's services equivalent. In such circumstances, data controllers would also have to necessarily keep monitoring market developments in order to ensure the continued validity of consent for their data processing activities, as competitors may alter their service at a later stage.

As a result, the EDPB states that a consent that relies on an alternative option offered by a third party must be deemed in violation with the GDPR. content from being visible, except for a request to accept cookies and the information on which cookies are being set and for what purposes data will be processed. In such a case there is no possibility to access the content without clicking on the 'accept cookies' button, meaning that the data subject is not presented with a genuine choice. Therefore, consent is not freely given, and cannot be deemed valid, as the provision of the service relies on the data subject consent to the placement of cookies.

Consent as an unambiguous indication of wishes

The EDPB is of the idea that consent under the GDPR must always be given through an active motion or declaration, and that It must be obvious that the data subject has consented to the specific processing activity.

Therefore, the EDPB, as per Recital 32 of the GDPR, find that scrolling or swiping through a webpage, or similar user actions,

will not in any case constitute a clear and affirmative action, since it may be difficult to distinguish such actions from other activity or interaction of the user. Thus, in such a case determining that unambiguous consent has been obtained will not be possible, and it will also be difficult to provide a way for the user to withdraw consent in a manner that is as easy as granting it.

Planet49 Judgment

The CJEU established that a pre-filled cookie banner which the user must deselect to refuse consent is not considered lawful. In fact, valid consent to cookies requires an active and specific indication of the website visitor's wishes. The judgment also states that the interpretation of the ePrivacy Directive does not have to change depending on whether the information stored or accessed through cookies constitutes personal data. The Planet49 case also confirms that the cookie notice must include information on both the lifespan of cookies and third parties' access.

UK - ICO Guidance on Cookies - Key Recommendations

- Continue browsing on the website is not a valid way of expressing consent.
- Do not bundle consent into general terms and conditions or privacy notices. In fact, the request must be separate from other matters.
- Analytics cookies are not strictly necessary. Therefore, they require consent.
- Cookie walls are not allowed.
- 'Nudging' designs in the consent mechanism aimed at influencing the user's choice are not allowed.

France - CNIL Revised Guidelines on Cookies and Online Trackers and finalized Recommendations - Key Recommendationss

- Continue browsing, pre-filled banners, and general terms and conditions are not valid ways of obtaining consent.
- Any inaction or action other than a positive one must be considered as refusal, and non-strictly necessary cookies cannot be placed.
- Cookie walls are likely to undermine the freedom of users to consent. However, following the Conseil d'Etat decision invalidating the CNIL former guidelines, cookie walls, although not banned in the revised guidelines, must be assessed on a case-by-case basis. In practice, if a cookie wall is set up, and subject to the lawfulness of this practice, the information provided to users must clearly indicate the consequences of their choice, with specific reference to the impossibility to access the content or service if consent is not provided.
- Users must be presented with both the possibility of consenting and refusing cookies with the same degree of simplicity. Therefore, presenting the user with two buttons on the 1st layer ('accept all' and 'refuse all') is recommended.
- Refusal of cookies may result from different actions, such as by simply closing the banner or by not interacting with the same for a certain period of time.
- Misleading design practices suggesting users that their consent is required or visually highlighting one choice over the other are not allowed.
- The data controller must be always able to demonstrate the collection of valid consent through adequate mechanisms, such as keeping a screenshot of the visual rendering in a time-stamped manner.

- CNIL recommends highlighting every purpose of cookies in the first layer with a short and prominent title, followed by a brief description. A more detailed description of the purposes will then be easily accessible from the first layer, through a drop-down button or a direct link.
- In the case of third party cookies allowing the user to navigate beyond the website/app on which they are initially installed, it is strongly recommended to obtain consent for each website/app visited by the user, so that the latter can be entirely aware of the scope of the consent he provided.
- For the demonstration of a valid collection of consent, the mere presence of a contractual clause between publisher and third party committing one to obtain consent on behalf of the other is not sufficient. Such clause should be amended to specify that the subject collecting consent must make available to other involved parties the proof of the same, so that each actor is able to demonstrate the lawful collection if needed.
- Users' preference/choice (consent or refusal) may be retained for a period of 6 months.
- Audience measurement and others analytic cookies may be regarded as strictly necessary and thus can be exempted from the collection of consent.
- Audience measurement cookies must be retained for a maximum period of 13 months, while information collected through them should be retained for a maximum period of 25 months.
- CNIL provides for a grace period of 6 months from the publication of finalized recommendations. Organizations must be compliant by the end of March 2021.

Germany - DSK Guidance on Telemedia Providers - Key recommendations

- Consent is not the only legal basis for cookies. The performance of a contract or the legitimate interest of the data controller or a third party are further possible legal bases for setting cookies.
- Cookie banners merely providing an 'OK' button, with no option to refuse the setting of cookies are not considered lawful.
- The lifespan of cookies is not specified under German law. However, the DSK recommends a short lifespan.
- Analytic cookies are usually strictly necessary and do not require consent.
- Cookie walls are not allowed.

Germany - DSK Guidelines on the Use of Google Analytics in the No-Public Sector

The guidelines complement the Guidance on Telemedia and provide that:

- Google Analytics can, in its current form, no longer be considered a data processor, but rather a (joint) data controller.
- The data collected through Google Analytics does qualify as personal data according to Article 4(1) of the GDPR.
- Therefore, website providers using Google Analytics need to get free, informed, and positive user consent to the use of Google Analytics.
- Website providers must ensure that consent can be easily withdrawn and provide a clear privacy policy, respect the principle of transparency, and use the option to shorten IP addresses.

Germany - BGH Decision Following CJEU Planet49 Judgement and DSK Reaction

The German Federal Court of Justice ('BGH') issued, on 28 May 2020, its final decision on the case that was previously suspended in favour of a preliminary ruling procedure of the CJEU in the Planet49 case. In particular, the BGH based its decision on the Planet49 Case and confirmed that pre-ticked checkboxes do not fulfil the requirements for consent and are unlawful. Furthermore, the BGH decided that Section 15(3) of the Telemedia Act (TMG) is to be interpreted in conformity with Article 5(3) of the ePrivacy Directive.

In addition, the DSK issued, on 26 November 2020, a resolution calling the Federal Legislature to fully implement Article 5(3) the ePrivacy Directive in the German legislation, considering that, following the Planet49 case, opt-out consent can no longer be deemed validly obtained under the GDPR.

Spain - AEPD revised Guide on the Use of Cookies - Key Recommendationss

The AEPD guide was updated on 28 July 2020 in light of the EDPB's revised Guidelines on Consent under the GDPR. The AEPD specified that the revised guide must be implemented by no later than 31 October 2020.

The guide recommends the presentation of information on cookies through layers. The first layer must contain essential information, while the second presents more detailed indications on the use of cookies.

- The mere consultation of the second layer of the cookie policy cannot be deemed as a valid way of expressing consent.
- A user navigating a website in order to manage his/her cookie preferences is not providing valid consent.

- Continued browsing, scrolling or navigating cannot be considered a clear affirmative action under any circumstances. Therefore, these actions may no longer be considered a valid way to obtain consent, in accordance with the EDPB Guidelines on consent under the GDPR.
- Following the EDPB's Guidelines on consent under the GDPR, cookie walls cannot be used, since they do not offer a valid alternative to consent. This is of particular importance in cases where the denial of access would prevent the exercise of a right legally recognised to a user, such as when access to a website is the only means provided in order to exercise the right. However, there may be certain circumstances where not accepting cookies shall entail being entirely or partially prevented from using the service, given that appropriate information is provided to the user and that an alternative access to the service is granted without the need of accepting cookies. The alternative service must be genuinely equivalent, and it will not be considered as valid if it is offered by a third party different from the publisher.
- Analytic cookies require consent.
- The AEPD considers good practice a validity period of no longer 24 months for user's consent.
- The website provider may collect consent for services offered in different domains through a single website, if the services present similar characteristics.

What Are the Language Requirements for Cookie Notices and Privacy Policies in the EU?

In order to respect the principle of transparency, as provided by article 5(1)(a) of the GDPR, which requires any processing of personal data to be to be carried out 'in a transparent manner', Article 7(2) of the GDPR provides that if the data subject's consent

is given in the context of a written declaration, the request for consent shall be presented using clear and plain language. Article 12(1) of the GDPR also requires the controller to take appropriate measures to provide any information referred to in Articles 13 and 14 of the GDPR in a concise, transparent, intelligible, and easily accessible form, using clear and plain language.

In addition, the WP29, in its Guidelines on transparency, recommends the data controller to ensure that, when the data controller provides privacy notices in different languages, the translations are accurate and reflect each other in the content. The WP29 also suggests translating the privacy notice in the language of the targeted data subjects.

European regulators also expressed their view on the language requirements of privacy notices and cookie policies.

For example, the Spanish AEPD guide on cookies addresses the topic of cookie policy transparency in relation to third parties. In particular, it says that, when the website publisher provides information about third-party cookies through a link to a third party website, it must ensure that the third party is responsible for ensuring that any information provided by such links is displayed in Spanish or in any other language with co-official status in Spain.

In addition, the Belgian data protection authority provides that the information included in the cookie policy must be written in a language easy to understand for the targeted audience. In practice, if the website is aimed at a French-speaking and/or Dutch-speaking audience, the information must be provided in French and/or Dutch.

Ireland - DPC Guidance Note on Cookies and Other Tracking Technologies - Key Recommendations

- Devices using cookies may also include Internet of Things devices connected to the internet.
- Both first-party and third-party analytic cookies require consent.
- Continue browsing on the website, either through clicking, using, or scrolling, is not a valid way to obtain consent.
- When the website publisher uses a third-party Consent Management Provider (CMP), the following apply:
  - The tool or software must not contain pre-checked boxes for the use of cookie.
  - When the CMP tool keeps a record of users' consent, the publisher must also keep a record of that consent under Article 30 of the GDPR.
  - The collected consent is valid for no longer than 6 months, and it must be re-collected afterwards.
- The interface of the cookie banner cannot 'nudge' the user into accepting cookies over rejecting them. At the same time, accessibility must be considered when designing interfaces.
- The DPC provided for a grace period of 6 months, and enforcement commenced from October 2020.

Part 3: CCPA Requirements, Rights and Terminology

The California Consumer Privacy Act (CCPA)

The California Consumer Privacy Act came into effect on January 1 2020. This law grants all consumers new rights to notice and

choice about the personal information that businesses collect and how they use or sell their personal data.

Unlike EU data protection law, CCPA covers only for-profit entities ('businesses'). Overall, its scope is limited to commercial activities. CCPA can be interpreted to cover businesses that are established outside California if they collect or sell California consumers' personal information.

The CCPA protects "consumers" who are natural persons and who must be California residents. Under this law, when businesses are collecting personal information of consumers based in California, they must disclose to consumers what information is being collected and for what purposes, whether they plan or intend to sell their personal information, to whom, etc. The operationalization of these new obligations varies depending on the context.

Terminology

Personal Information

Personal Information is broadly defined in §1798.140(o)(1) of CCPA as 'any information that relates to, describes, is capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular California consumer, [device] or household.' CCPA lists a non-exhaustive catalogue of examples of what is considered personal information:

- Identifiers, such as name, alias, postal address, IP address, email address, social security number, driver's license number, passport numbers, professional credentials, inferences drawn (profiling), education information, etc.
- Commercial information, such as records or personal properties, consumer tendencies, articles purchased, etc;

- Biometric information;
- Internet or other electronic network activity information, including browsing history and information about a users' interaction with a website, mobile application or digital advertisement, hence tracking technologies such as cookies:
- Geolocation data;
- Audiovisual data;
- Olfactory, thermal, electronic or similar information.

Although cookies are not directly addressed in CCPA, they are interpreted to be encompassed in this wide definition of personal information under 'internet and other electronic network activity'.

Exceptions

As broad a definition as this is, §1798.140(o)(2) lists three types of information that are not considered personal information: publicly available information, aggregate consumer information, and de-identified information.

- Publicly available information means information that is lawfully made available from federal, state or local government records. For data to be considered publicly available, the purpose for which the information is used has to be compatible with the purpose for which the data is maintained and made available.
- Aggregate consumer information means information that relates to a group of consumers from which individual identities have been removed and that is neither directly linked nor can be reasonably linked to a consumer or household. This should not be confused with de-identified information.
- De-identified information means data that cannot reasonably

identify, relate to, describe, be capable of being associated with, or linked directly or indirectly to an individual consumer because the information has been anonymized. Businesses using de-identified data must:

- Implement technical safeguards that prohibit re-identification;
- Implement businesses processes that specifically address and prohibit re-identification;
- Implement businesses processes that specifically aim at preventing the release of de-identified information;
- Prevent any attempt to re-identify the information.

Business

CCPA imposes obligations on commercial entities that meet three requirements laid down in 1798.140(c)(1):

- Do business in California:
- Are operated for the profit or financial benefit of their shareholders, and:
- Collect consumers' personal information and determines the purpose and means of the processing of those data

Besides these three requirements, for businesses to be covered by CCPA they must satisfy one or both of these two thresholds:

- Have an annual gross revenue in excess of twenty-five million dollars; or
- Alone or jointly process personal information of 50,000 or more California consumers, households or devices (i.e. any physical object that can connect to the internet or to another device).

Sale

§1798.140(t)(1) of CCPA defines "sale" quite broadly: it means 'selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by the business to another business or a third party in exchange for a monetary or other valuable consideration'. A valuable consideration from this point of view could mean a monetary exchange or a non- monetary consideration such as, for example, the provision of services or in-kind exchanges.

The three main elements of the definition of a "sale":

- A sale must involve Personal Information as defined in CCPA. If the operation in question involves de-identified information, publicly available information, or aggregate consumer information said operation would not involve Personal Information.
- Movement or transfer of Personal Information from one business to another, or to a third party. For example, making a cookie ID available to a third party through real-time bidding – when this cookie relates to a consumer, a device or a household.
- Consideration is defined in California case-law as a "bargained-for exchange", whereby the exchange of (e.g.) Personal Information in return for something of value is the main intention. If the transfer of personal information is just an incidental consideration, said transfer would not constitute a sale.

These elements are cumulative and they all must be present when a business is selling Personal Information. To be able to comply with CCPA, it is important to understand when a move of personal information constitutes a "sale".

Exceptions

CCPA specifies four scenarios where personal information is being transferred from one business to another but where such movement of personal information does not constitute a" sale":

- Communicating opt out preferences: this applies where a business shares personal information with a third party to alert them of the consumer's opt out preferences.
- Intentional interaction with a third party: a business does not sell personal information if the consumer has directed the business to intentionally disclose their information or uses the business to intentionally interact with a third party.
- Mergers, acquisitions and other corporate sale transactions: this happens where a third party takes control of all or part of the business, and personal information is transferred as an asset as part of that transaction.
- A business purpose: which is defined as "a business's or a service provider's operational purposes, or other notified purposes". To be covered by this exception, transfers of personal information to third parties must fulfill four requirements:
    1. Necessity of the transfer: the transfer must be necessary to perform a task that has a "business purpose".
    2. Pursuant to a written contract that prohibits the service provider from "selling, retaining, using, or disclosing the personal information".
    3. Notice to consumers: the business has provided compliant notice to consumers of the fact that it intends to share with service providers.
    4. Limitation: the service provider does not further "collect, sell, or use" the personal information of the consumer except as necessary to perform the "business purpose."

The business purpose exception covers a wide array of standard business activities such as security and fraud prevention, auditing, internal research and service improvement, marketing, analytics, system security, as well as mere “short-term, transient use”. It also includes performing services provided on behalf of a business, such as maintaining customer accounts, processing orders or providing advertising or marketing services.

CCPA and Cookies

In its definition of Personal Information, CCPA includes a non-exhaustive list of identifiers and types of information that are of a personal nature, including the term “unique identifier”. §1798.140(x) of the CCPA indicates that a unique identifier is ‘a persistent identifier that can be used to recognize a consumer, a family, or a device that is linked to a consumer or family over time and across different services’.

Examples of “unique identifiers” in CCPA include IP addresses, cookies, beacons, pixel tags, mobile ad identifiers and similar tracking technologies. It is not clear however if cookies are considered a stand-alone identifier or if they are just listed as an example of a technology that has the potential to recognize a device or a user overtime and across services.

If the information collected and processed using cookies – or other tracking technologies – can be reasonably linked to a consumer, household or device, said processing must comply with CCPA rules.

Especial attention must be paid to practices such as behavioral advertising using tracking technologies. This type of processing could constitute a sale of personal information (e.g.) by enabling third party cookies on a website that allow those parties to read and or write information contained in the cookies.

Consumer Rights

CCPA protects several rights of California consumers, some of which are parallel to GDPR data subject rights. CCPA protects the right to receive information; the right to request (obtain) information from businesses that are processing personal data, or right of access; the right to deletion; the right opt-out of the sale of Personal Information; the right to not be discriminated for exercising consumer rights; and the right to data portability.

Below we review the right to receive information, and the right to opt-out in the context of cookies. They are the baseline themes for compliance with CCPA in a digital context where unique identifiers are being enabled. All other rights are important for compliance, but an in-depth analysis of every CCPA consumer right is out of the scope of this handbook.

The right to receive information and the right of access

§1798.100(b) of the CCPA imposes on businesses that collect and process personal information the obligation of transparency. Businesses must inform consumers of:

- the information collected; and
- the processing purposes.

This information must be provided before or at the time of collection. Unlike the GDPR, CCPA does not draw a line between direct collection of information from the data subject, and indirect collection through other sources. This means that the same timeframe should be respected, and the same amount of information should be made available to consumers before or at the time of collecting the data (e.g. before enabling cookies) regardless of the source.

Subparagraphs (A) and (B) of paragraph (5) of subdivision (a) of §1798.130 stipulate that, in order to comply with the transparency obligation, where businesses have a website they must also disclose in their online privacy policy a description of all consumer's rights; and, a list of the categories of personal information that have been collected in the preceding 12 months. Businesses that sell Personal Information must include two separate lists in their online privacy policy:

- a list of categories of personal information sold in the preceding 12 months (or any lack of thereof); and
- a list of categories of personal information that was disclosed for a business purpose in the preceding 12 months (or any lack thereof).

In addition, when businesses sell personal information §1798.135(a) imposes the obligation to include a California-specific description of consumers' privacy rights. Website publishers should inform users and enable them to exercise their right to opt-out of the sale of their personal information.

In a digital context where cookies are enabled, this is typically achieved with a cookie notice and other mechanisms such as banners providing layered information using conspicuous links.

The right to opt-out of the sale of personal information

§1798.120(a) indicates that A consumer shall have the right, at any time, to direct a business that sells personal information about the consumer to third parties not to sell the consumer's personal information. This means that businesses that sell Personal Information must provide a clear and conspicuous link titled "Do Not Sell My Personal Information" on:

- their homepage;
- any webpage where you collect personal information;
- mobile app's iOS/Android;

- their privacy notice; and
- in any other document or page describing the rights of California consumers.

This link must re-direct consumers to an Internet Web page that enables them to opt out of the sale of their personal information.

§1798.120 stipulates that after consumer has exercised the right to opt-out, businesses are prohibited from selling that consumer's personal information from that point forward, unless they receive express authorization from the same consumer for the sale of his or her Personal Information. Businesses must wait 12 months from the moment a consumer opted out in order to it subsequently receives express authorization from the consumer for the sale.

§1798.135 (a) (5) indicates that businesses can request consumers to opt back in, but they must respect the consumer's decision to opt out for at least 12 months before asking the consumer to opt in.

To clarify, the opt out continues past the twelve-month period, the twelve-month period is only significant in that it represents the time that must pass for a company to try to gain a consumer's consent to sell personal information again.

Minors between the age of 13 and 16 must be offered the possibility to opt-in, that is, to consent to their sale of their personal information before any transfer takes place.

In California, third parties that receive personal information are allowed to resell those data provided that consumers have received explicit information about the potential resale and are provided with a timely opportunity to exercise their right to opt-out of that resale.

The Attorney General in California was required to promulgate regulations to clarify and operationalize the CCPA. In general

terms, the regulations that have been adopted by the Attorney General establish rules and procedures for the following:

- To facilitate and govern the exercise of the right to opt out of the sale of personal information.
- To regulate business compliance with consumers' requests to opt-out.
- To promote consumer awareness of the right to opt out by standardizing opt-out icons or buttons.

CCPA Cookie Banner Best Practices

A CCPA cookie banner should include the following:

- Information about cookie use that includes details about the purpose for the use of cookies on the site and whether the site shares the information with third party companies.
- A button to accept or decline cookies. Although the CCPA doesn't require consumers to opt-in to cookies before the website can drop cookies, it's considered best practice to still inform the user about the data it collects. The cookie banner can include a link to a cookie settings page where a user can choose to opt-in or out, as well as see exactly what cookies they're consenting to.
- The CCPA requires that businesses include a link or button to an opt-out form on your home page. The button should read "Do Not Sell My Personal Information." The link needs to route to a "Do Not Sell" page on your website. The Do Not Sell page should include a link to a privacy policy and the option to opt-out of personalized advertisements. This button is not considered a cookie banner, but it can be on or near the cookie banner – see the example below. Read more about how to comply with the CCPA Do Not Sell Rule in this blog post.

- The consumer must have the ability to withdraw consent for the sale of their personal information at any time in an easy-to-find spot on the website.

Operationalization of the Right to Opt Out

The Interactive Advertising Bureau ('IAB') and the IAB Tech Lab released technical specifications associated with the IAB California Consumer Privacy Act Compliance Framework for Publishers and Technology Companies. The Framework applies to RTB transactions involving the "sale" of Consumers' personal information only when all participants in a transaction are Framework Participants. This Framework is flexible in that Publishers that choose not to participate can still send the same signals to downstream technology companies of their choosing.

This Framework was created as a multi-stakeholder effort with the dual aim of:

- creating a service provider relationship between publishers and tech companies; and
- providing publishers and tech companies who sell personal information with a mechanism for limitation and accountability to be implemented when consumers opt out of a sale of PI.

This framework is created for publishers and tech companies to streamline consent – or lack thereof – to the sale of consumers' Personal Information.

There are two main outcomes after a consumer opts-out of the sale of Personal Information:

- the sale of personal data must cease; and
- the wishes of consumers will be effectuated through a Limited Service Provider Agreement that has to flow downstream to tech companies within the value chain.

Although the Framework is primarily aimed at businesses that sell PI, the creation and facilitation of service provider relationships makes the Framework suitable for its use by businesses that do not sell PI.

The main benefits of this Framework are:

- It facilitates an efficient vehicle for the creation of service provider relationships in the ecosystem; and
- Provides a mechanism to demonstrate accountability for participants in the Framework, by requiring them to submit to audits to ensure that when the consumer opts-out, limited personal information is only being used for permitted business purposes under CCPA (e.g. auditing, detecting security incidents, short term transient use, etc.).

Part 4: OneTrust Solutions

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 publisher s needs 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 publishers 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 enables instant updates to changes 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 publishers the power to provide granular controls for visitors, respecting their preferences while ensuring the website publisher'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 5: OneTrust FAQs

Do we need a cookies' scanning tool, a cookie preference centre, or a cookie policy explaining the cookies used on the website?

As outlined by the recommendations above, organizations must implement appropriate measures in order to provide the user with transparent information, so that the individual will be able to provide a lawful consent to the setting of cookies and similar technologies, in accordance with the ePrivacy Directive and its implementation legislations.

Does OneTrust have a solution for the IAB TCF?

The IAB Europe's Transparency and Consent Framework ('TCF') is a GDPR consent solution built in order to create an industry-standard approach. The objective of the TCF is to help all parties in the digital advertising chain ensure that they comply with the GDPR and the ePrivacy Directive when processing personal data or setting cookies and other tracking technologies.

The TCF creates an environment where website publishers can tell visitors what data is being collected and how their website and companies they partner with intend to use it. In addition, the TCF addresses, among other things, the presence of CMPs as an instrument to lawfully obtain and record consent.

Recently, IAB Europe announced the launch of its TCF v2.0. In particular, the TCF v2.0 introduced several improvements in order to:

- Enable consumers to grant or withhold consent, as well as to exercise the 'right to object' to data being processed;
- Enable consumers to gain greater control over whether and how vendors may use certain features of data processing, for

example, the use of precise geolocation; and

- Enable publishers to gain extended control and flexibility with respect to how they integrate and collaborate with their technology partners.

In relation to CMPs, the TCF v2.0:

- Enable CMPs to capture, store, and signal consent in an industry-standard manner;
- Enables CMPs to receive global consents obtained by other publishers and CMPs;
- Records which vendors are operating in the TCF and the purposes that they wish to process personal data for, in order to update the user interface and inform users accordingly; and
- Informs CMPs when vendors use legitimate interest or consent as a legal basis for processing personal data, so that users can be informed accordingly.

OneTrust, after working closely with IAB Europe, recently announced that the OneTrust Consent Management Platform (CMP) is officially TCF v2.0 approved. Publishers can use the OneTrust CMP to switch to v2.0, and access resources, tools, and templates only available to OneTrust customers. OneTrust recently launched a free tool for publishers to build and deploy an IAB Transparency and Consent Framework v2.0 (TCF 2.0) CMP for free and in just a few steps.

What is the territorial scope of the ePrivacy Directive? Does the establishment of the organisation running the website, the location where data is hosted, the place where the majority of traffic is coming from, or the market of the website, play a role in the identification of the national applicable legislation?

The ePrivacy Directive does not have any provisions that expressly set out its geographical scope of application. However, its relationship with the GDPR must be considered in order to understand its territorial scope of application.

Firstly, it must be considered that Article 94 of the GDPR repeals the old Data Protection Directive and provides that any reference to the repealed Directive shall be construed as references to the GDPR.

The ePrivacy Directive must be thought of as a specialised subset of rules falling under the broader privacy framework established by the GDPR.

In fact, Recital 10 of the ePrivacy Directive provides that, with reference to the electronic communications sector, Directive 95/46/EC [now GDPR] applies to all matters concerning protection of fundamental rights and freedoms, which are not specifically covered by the provisions of Directive 95/46/EC [now GDPR], including the obligations on the controller and the rights of individuals.

And Article 1(2) of the ePrivacy Directive also states that the provisions of the ePrivacy Directive particularise and complement Directive 95/46/EC' [now GDPR].

Therefore, since the ePrivacy Directive does not expressly address its territorial scope of application, Article 3 of the GDPR, regulating its territorial scope, acquire relevance in the context of the ePrivacy Directive.

The EDPB Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR stated that the use of cookie triggers the application of both the ePrivacy Directive and the GDPR. Therefore, when the use of cookies implies the processing of personal data, the GDPR, and its territorial scope as a consequence, will find application.

The EDPB further outlined that, for the ePrivacy Directive to be applicable, the service and network must be offered in the EU. In addition, it stated that Articles 5(3) of the ePrivacy Directive not only apply to providers of electronic communication services, but also to website operators or other businesses.

Lastly, Article 3 of the ePrivacy Directive states that its application will cover any processing of personal data carried out in connection with the provision of publicly available electronic communications services in public communications networks in the Community.

How does implicit consent pan out with the wider EU approach to valid consent with recent case law?

Recent case law as well as several recommendations and guidelines of regulators across Europe, have deemed implied consent too vague to fulfill the strict sine qua non elements of consent as required by the GDPR. For example, users can continue to navigate a website (e.g. by clicking on the “about” tab instead of closing the window) by mistake. Some devices are quite sensitive and clicking on a website by mistake while dragging the cursor is quite common. In fact, many phishing attacks on the web

rely on user mistakes for purposes such as getting a click on an ad to obtain users' credentials. In an offline/analogue setting, implied consent can indeed work, because there are visible actions that are unmistakably interpreted as consent (e.g. taking something from someone's hand without saying a word). In this respect, the ICO is of the opinion that in an analogue setting an affirmative action is solid enough for obtaining consent. However, the same may not hold true in an online context.

In addition, the trend of the CJEU has continued to be a strict view of what constitutes valid consent. For example, their decision in the case Planet49 requires a positive and unequivocal action consisting on clicking or switching or toggling preferences in order to interpret valid consent from users, boxes can't be pre-ticked because this would go against the positive action requirement for consent to be valid. By extrapolation, implied consent would not be upheld if such practice was challenged in court because it fails to pass a strict test of valid consent. For the time being, the Spanish regulator interprets this as an acceptable practice and can be carried out in Spain, provided that other essential elements of consent are fully respected. It is essential to have provided intelligible, unequivocal information to users before interpreting their actions as consenting to tracking technologies and purposes. Clicking on the privacy policy/cookie notice link is not valid implied consent.

Can the consent collected within one internet domain be used to place cookies through a separate domain, when both the websites are owned by the same subject? In other words, can consent be transferred among websites developed by the same entity?

In relation to different internet domains owned by the same subject, several European regulators are of the view that the consent obtained for one website can be used for other websites as well, if certain conditions are respected.

For example, the Spanish regulator's view is that the single website providing services across different domains may use the same consent if the different domains display similar characteristics and are used for the purpose of providing services requested by users. The website must also inform the users about the websites or domains that are held by the same website provider. Lastly, in case the website provides different services and display characteristics or offer contents which are not similar, additional precautionary measures must be implemented.

In addition, the Dutch supervisory authority notes that, if the user has been informed about the intended us of cookies and about different domains, the user's consent may be valid for multiple domains. The user must also be offered the opportunity to browse through a comprehensive list of domains, so that there has been a free and specific expression of will. The bundled consent must reasonably be an expectation for the user, and the websites must offer the same type of service.

Lastly, the Italian supervisory authority provides for the same requirement, but in relation to the cookie policy. The website can provide a single cookie policy for different websites. The cookie policy must contain an always updated list of all the domains in which the processing is carried out through cookies.

Is the cookie legislation applicable to organizations' intranet, for example in the employment context?

Article 3 of the ePrivacy Directive states that:

'This Directive shall apply to the processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks in the Community, including public communications networks supporting data collection and identification devices.'

The EDPB Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities outlines that the ePrivacy Directive applies when each of the following conditions are met:

- there is an electronic communications service;
- this service is offered over an electronic communications network;
- the service and network are publicly available;
- the service and network are offered in the EU.

Examples of activities which do not meet all of the above criteria and are generally out of scope of the ePrivacy Directive:

- [A corporate network which is accessible only to employees for professional purposes does not constitute a 'publically available' electronic communications service. As a result, the transmission of location data via such a network does not fall inside the material scope of the ePrivacy Directive].

Is there any guidance to rely on in relation to cookies retention? How should organizations address the principles of necessity and proportionality within their business functions?

In relation to the European landscape, as the storing of cookies or similar tracking technologies imply the processing of personal data in most of the cases, the GDPR's provisions related to data retention must be taken into account. In particular, although the GDPR does not provide for specific retention periods in relation to personal data, Recital 39 and Article 5(1)(e), introducing the principle of storage limitation, states:

'The personal data should be adequate, relevant and limited to what is necessary for the purposes for which they are processed. This requires, [...] ensuring that the period for which the personal data are stored is limited to a strict minimum. [...] In order to ensure that the personal data are not kept longer than necessary, time limits should be established by the controller for erasure or for a periodic review'.

'Personal data shall be [...] kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed [...]'.

Therefore, when processing personal data through the use of cookies or other similar technologies, a data controller must retain the data for a period that must be balanced with the purpose of the processing and cannot be retained for longer than what is necessary to achieve the purpose of the processing. In this regard, an assessment of the principles of necessity and proportionality to the specific circumstance is key for organisations using cookies. In practice, the data controller must be sure that the use of cookie is proportionate in relation to his/her intended outcome and limited to what is necessary to achieve the purpose of processing. In any case, the data controller will also need to be able to justify the necessity of a given retention period, according to the principle of

accountability.

From a business perspective, organisations should also consider that implementation of retention periods will reduce the risk that it becomes irrelevant, excessive, inaccurate or out of date. In addition, holding more personal data than what is needed may be inefficient, and as a result, operators might face unnecessary costs in relation to storage and security.

With specific reference to cookies and similar technologies, there is not a pan-European cookie retention period prescribed by law. However, several European regulators have provided more detailed guidance on the topic, offering organisations indications for the application of the general principles.

In this regard, a distinction must be drawn between cookies requiring the consent of the user and cookies that are exempted from this requirement, in accordance with the ePrivacy Directive. In relation to cookies not requiring the user's consent, the former WP29 recalled in its Opinion 04/2012 on Cookie Consent Exemption that exempted cookies should have a lifespan that is directly related to the purpose they are used for, and must be set to expire once they are no longer needed, taking into account the reasonable expectations of the average user. This suggests that these cookies should be likely be set to expire when the browser session ends, if not earlier.

However, the WP29 also reminds that, while login cookies are typically set to expire at the end of a browser session, cookies aimed to ensure the user's security are expected to have a longer lifespan in order to fulfil their security purpose.

Organisations must also keep in mind their transparency obligations in relation to the retention of cookies. The CJEU upheld in the Planet49 case that the cookie notice must include, among other things, information on the lifespan of cookies. In fact, the duration of the operation of cookies must be deemed

as included in the clear and comprehensive information which must be provided to the user in accordance with Article 5(3) of the ePrivacy Directive. In addition, it must also be recalled that Article 13(2)(a) of the GDPR provides that the controller must, in order to ensure fair and transparent processing, provide the data subject with information relating, inter alia, to the period for which the personal data will be stored, or if that is not possible, to the criteria used to determine that period.

Lastly, organisations should also take into consideration that certain EU Member States' data protection authorities produced guidance in relation to cookies retention, offering a non-harmonised outlook in terms of prescribed periods. Therefore, organisations must consider, on the basis of their business location, coverage, and audience, the differences between the different regulators' guidelines. Some of this key guidance on cookies retention is discussed briefly below.

Belgium

The DPA highlights that cookies stored on the user's terminal equipment cannot be stored beyond the period necessary to achieve the intended purposes. Therefore, the retention period must not be set as indefinite, and must also take into account the reasonable expectations of the user. Information collected and stored in a cookie, as well as information collected following the access of a cookie, should be deleted when they are no longer necessary in relation to the purposes of processing.

France

CNIL provides that, in relation to audience measurement cookies, they must not have a lifespan exceeding 13 months, and this period must not be automatically prolonged. In addition, information collected by the above cookies must be retained for a

maximum period of 25 months.

CNIL also notes that the user's preference/choice (consent or refusal) may be retained for a period of 6 months.

In this regard, CNIL provides that websites, which generally keep the consent for a certain period of time, also should keep in the same way the refusal of users, in order not to re-interrogate the user at each visit. In fact, failure to keep users' choices would result in users being presented with a new banner on every visited webpage, which would affect the freedom of their choice.

Germany

The DSK Guidance on Telemedia Providers states that shorter lifespans are more likely to meet the requirements of the balance of interests test between service providers and users under Article 6(1)(f) of the GDPR.

Ireland

The DPC Guidance Note on Cookies and other tracking technologies provides that the expiry date of a cookie should be proportionate to its purpose. Session cookies, for example, which are designed to only function for the duration of a browser session or slightly longer, are likely to have a very short lifespan and to be set to expire once they have served their limited purpose.

Spain

Cookie retention periods are not provided in the law. However, the AEPD recommends renewing users' consent at regular intervals. In particular, it is considered good practice to consider the consent granted by users regarding a specific cookie valid for a period of no longer than 24 months. During this time, users' preferences

may be stored so they are not asked to set them up again every time they visit the relevant page.

UK

The ICO recalls that cookie retention depends on the purpose of the cookie. It must be ensured that the use of cookie is proportionate in relation to the intended outcome and limited to what is necessary to achieve the purpose of processing, which is likely to lead towards the determination of the duration.

Can users' cookie preferences be propagated across platforms (e.g. mobile, browser)?

As outlined in the Handbook, publishers use cookies in order to optimize users' searches on the basis of their search history and on results they have been selecting, as well as to tailor their digital advertising activities. This practice, with the increased use of mobile devices to access the internet, faces new challenges with a relevant impact on organisations' practices, since the mobile environment entails new challenges comparative to browsers and personal computers. Whilst mobile applications and mobile browsers operate on the same physical device, they represent more isolated ecosystems than computers' browsers, and website owners can find more difficult in identifying a user as the same subject when using different apps or the mobile browser. As a result, cookies and other similar technologies, when installed on mobile, may be less effective than on traditional personal computers.

From a European standpoint, it must be noted that the ePrivacy Directive does not provide for a definition of 'terminal equipment'. However, the proposed Draft ePrivacy Regulation considers the

definition offered by the Commission Directive 2008/63/EC of 20 June 2008 on competition in the markets in telecommunications terminal equipment, which defines 'terminal equipment' as:

'[...] equipment directly or indirectly connected to the interface of a public telecommunications network to send, process or receive information; in either case (direct or indirect), the connection may be made by wire, optical fibre or electromagnetically; a connection is indirect if equipment is placed between the terminal and the interface of the network [...]'.

In addition, the WP29 highlighted in its Opinion 02/2013 on Apps on Smart Devices that apps access data stored on the device, contacts in the address book, pictures, videos and other personal information. Therefore, Article 5(3) of the ePrivacy Directive, requiring consent from the user on the basis of clear and comprehensive information, is to be considered applicable. Therefore, it can be stated that the ePrivacy Directive applies to both personal computer browsers and mobile environments.

The cross-validity of cookie consent represents a topic that yet to be analysed in detail through regulators' guidance and recommendations. However, some of the main data protection authorities, as well as industry organizations, have addressed mobile and cross-mobile consent as a whole in recent guidelines and frameworks, providing organizations with indications on best practices to be put in place in order to ensure a compliant approach.

For example, the ICO confirmed in its guidance that the use of cookies and similar technologies is not limited to traditional websites and web browsers, but also apply to mobile apps. The ICO notes that web application programming interfaces (APIs) are typically used by mobile devices and other hardware, and that they can also store or access information on the user's device. Consequently, the ICO underlines that the mobile app accessing

the web API is the place where publishers must incorporate the consent mechanism. However, the ICO recognizes that the limited, and sometimes non-existent, physical interfaces on some internet-connected devices pose challenges when trying to inform users about cookies and their purposes. In this regard, organizations must consider alternative methods of informing users, such as:

- clear instructions packaged along with the device;
- information provided during product registration; and
- the use of a companion mobile app to provide an interface so that information can be provided and consent gained.

In relation to the use of the cookie banner on mobile, the ICO recommends that organizations consider their implementation carefully, particularly in respect of implications for the user experience. For example, a message box designed for display on a desktop or laptop web browser can be hard for the user to read or interact with when using a mobile device, meaning that the consents obtained would be invalid.

Cookie requirements for mobile devices are also addressed by CNIL in its finalised recommendations on cookies. The recommendations confirm that they regulate trackers used by publishers on both websites and mobile applications. With reference to cross validity of consent, CNIL states that, in the case of third party cookies allowing the user to navigate beyond the website/app on which they are initially installed, it is strongly recommended to obtain consent for each website/app visited by the user, so that the latter can be entirely aware of the scope of the consent he provided.

The topic of mobile consent is also partially addressed by IAB Europe in its TCF Implementation Guidelines. In particular, when addressing the storage of consent, the Implementation Guidelines provide that, depending on the publisher preference and on the policy requirements, consent can be stored either locally or

globally through a 'shared' cookie. In addition, IAB Europe notes that CMPs are also free to store consent separately and with a different format if needed, provided that, if consent is being stored globally, they keep the shared cookie storing global consent up to date with their local changes.

However, the Implementation Guidelines further state that one of the most common methods for CMPs to store long term cookies is to do it on mobile, through internal data storage. In this regard, IAB Europe reminds that, although this method is easy to implement, affordable, and offers a good user experience, it also has limits, such as:

- it cannot be used as proof of consent; and
- it cannot be shared across apps, so device-wide consent may be difficult to achieve.

Lastly, the Implementation Guidelines suggest a combined approach between server-side storage, which enable to store consent for a long time and to share the same across apps, and client-side storage, for a local fast-to-access cache.

Can browser settings be considered a lawful way to collect consent?

The regulatory landscape regarding collection of users' consent through browser settings continues to be a topic of discussion. While there is a broad consensus from an EU legislative perspective, there does not appear to be a harmonized approach from a national standpoint, and still lacks practical recommendations on how to carry out this activity in compliance with the law. Therefore, organizations will have to keep in mind the flexible EU regulatory environment, as well as the varying recommendations issued by national authorities.

Further to the above, Recital 32 of the GDPR addresses the collection of consent through browser settings, even if not specifically in relation to cookies:

'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 [...]. This could include [...] 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'.

On the same, the EDPB specified in its Guidelines 05/2020 on Consent under the GDPR that obtaining consent from internet users via their browser settings is in principle allowed, as long as such settings are developed in line with the conditions for valid consent under the GDPR. Therefore, consent must be granular for each of the envisaged purposes and the information provided should include the identity of data controllers.

While the ePrivacy Directive does not address this topic, the Draft ePrivacy Regulation may allow the setting of cookies through technical settings in Article 4a(2) (here quoted in its last compromise proposal):

'[...] where technically possible and feasible, for the purposes of point (b) of Article 8(1), consent may be expressed by using the appropriate technical settings of a software placed on the market permitting electronic communications, including the retrieval and presentation of information on the internet.'

In relation to the above, the EDPS expressed its vision in Opinion No. 6/2017 on the Draft ePrivacy Regulation and stated that the expression 'where technically possible and feasible', as provided by the draft, is not sufficiently clear, and brings the risk of annulling the obligation itself through a too broad a range

of possibilities regarding interpretation. The EDPS therefore recommends that the phrase should be replaced by 'where technically feasible', in order to ensure legal certainty as to the scope of the obligation.

In addition, the EDPS also highlights that compliance with the principle of Privacy by Default is necessary. In practice, tools enabling the collection of consent through browser settings must be offered to the user with privacy-friendly default settings, both at the initial set-up and at any other moment when the user changes their devices or software.

From a national perspective, organizations may face different requirements as a result of national ePrivacy legislation, and as further interpreted by national regulators.

The Belgian data protection authority, for example, has noted that consent collected through browser settings is currently not compliant with the requirements of the GDPR. Consent in this form cannot in fact be sufficiently specific in relation to the purposes of the different types of cookies.

In France, although the national ePrivacy Law provides that consent may result from appropriate browser settings on a device belonging to the user, CNIL noted in its Guidelines on cookies that browser settings cannot, according to the current state of art, allow the user to express valid consent. In fact, the Guidelines note that nowadays web browsers, if one hand present users with the possibility to customize their choices in relation to cookies, on the other do not provide a sufficient level of prior information on the same, as well as do not allow to distinguish cookies on the basis of their purposes, which would be necessary to have a freely given consent.

The Irish DPC also stated in its Guidance on cookies that users' browser settings cannot be generally relied upon to infer consent for the setting of cookies, and that the circumstances where

browser settings are likely to be considered a valid tool to collect consent are very limited and would need to be assessed on a case-by-case basis.

Lastly, the data protection authority in the Netherlands welcomes user-friendly solutions enabling consent to be given in the browser settings. However, the regulator reminds organisations storing or accessing cookies that they cannot automatically assume that, if a browser accepts cookies, users must have given their consent to the same, since many browsers, by default, accept all cookies. Therefore, if the user has not amended the settings, it cannot be concluded that he/she accepts cookies.

What is the role that actors (publishers, CMPs, vendors etc.) of the ad tech ecosystem assume in relation to the concepts of data controller, data processor and joint controllership under the GDPR? In practice, what are the elements to be take into account when assessing the role and responsibilities of organizations operating in the ad tech environment?

The advertising technology (ad tech) ecosystem is a complex digital marketing environment consisting of each component necessary to manage digital advertising campaigns for demand and supply-side platforms. The ICO defines it in its Update report into ad tech and real time bidding as a set of tools that analyse and manage information (including personal data) for online advertising campaigns and for the automation of the processing of advertising transactions. The concept of ad tech covers the end-to-end lifecycle of the advertising delivery process, which often involves engaging third parties for one or more aspects of the services. In particular, the ad tech environment underpins real time bidding (RTB) as one of the most used programmatic advertising techniques (see the Part 1 of this Handbook for further information on RTB), where advertisers are allowed to compete for

available digital advertising space in milliseconds, placing online adverts on webpages and apps by automated means.

Where ad tech actors process personal data for the purpose of online advertising, the applicable data protection regulations will have to be taken into account. In particular, it can be challenging, within such a complex ecosystem, to understand and assign to subjects active in ad tech their data protection roles and responsibilities, as presented by the GDPR. In fact, the following several operators, among others, act within the ad tech ecosystem and share data among themselves for the purpose of targeted online advertising:

- Publishers/website operators
- Advertisers
- Ad network providers
- Advertising exchanges
- Demand side platforms (DSPs)
- Supply side platforms (SSPs)
- Data management platforms (DMPs)
- Consent management platforms (CMPs)

In this regard, although the European regulators produced recommendations on how to identify and appoint data controller, processors, and joint controllers under the GDPR, the practical application of this guidance to the ad tech environment is still partially unexplored.

The EDPB addresses the concepts of controller, processor and joint controllership in its Guidelines 07/2020 on the concepts of controllers and processors in the GDPR, currently under public consultation. However, the only reference to the advertising sector contained in the guidelines is in relation to certain processing activities that can be considered as naturally attached to the role

or activities of an entity. In this case, existing traditional roles and professional expertise that normally imply a certain responsibility will help in identifying the controller, such as in the case of a publisher processing the personal data of its subscribers. When the publisher processes personal data as part of its interactions with its own customers, it will have to be considered as the subject who factually can determine the purpose and means around the processing and will therefore act as a controller.

The role of ad tech actors is not otherwise mentioned in the guidelines and must therefore be reconstructed indirectly from the general definitions, as interpreted by the EDPB.

In addition, the WP29 addressed the roles of ad tech actors in relation to cookie obligations in its Opinion 2/2010 on online behavioural advertising, which, although referring to a pre-GDPR legal landscape, still presents elements of interest. Specifically, the WP29 provides recommendations in relation to the following subjects involved in behavioural advertising practices:

- Ad network providers
- Publishers
- Advertisers

Ad network providers: Considering that Article 5(3) of the ePrivacy Directive considers irrelevant whether the entity placing the cookie is data controller or processor, the WP29 considers ad network providers obliged to obtain the user's informed consent in the context of behavioural advertising. In addition, if the behavioural advertising activity entails processing of personal data, the ad network provider will assume the role of data controller. In fact, ad network providers:

- 'rent' space from publishers' web sites to place ads.
- set and read cookie-related information and collect other data that the browser may reveal.

- use the information gathered to build profiles and deliver ads.

Publishers: Publishers rent out space on their websites for ad networks to place adverts. In practice, they set up their web sites in a way that visitors' browsers are automatically redirected to the webpage of the ad network provider. Therefore, the WP29 notes that they should be aware that by entering into contracts with ad networks and providing them with visitors' personal data, they assume responsibility towards their visitors. The breadth of their responsibility, including the extent to which they become data controllers, should be analysed on a case by case basis depending on the particular conditions of collaboration with ad network providers, as reflected in the service agreements.

Advertisers: Advertisers can track the campaign resulted in the click-through when visitors click on ads and visit their website. When the advertiser captures certain targeting information, such as demographic data or an interest group, it can combine the same information with the data subject's onsite surfing behaviour or registration data. In this case, the WP29 outlines that the advertiser will assume the role of independent data controller for the relevant part of the data processing.

From a national standpoint, CNIL also addressed the roles and responsibilities of subjects involved in the use of cookies and similar technologies in its recently finalised recommendation on cookies. In particular, CNIL establishes that the publisher and the third party must be considered joint controllers for the placement of cookies when they jointly determine the purpose and means of processing, as clarified by the EU Court of Justice in the Fashion ID case. In this case, the two parties will have to establish their respective obligations under Article 26 of the GDPR, with specific reference to the collection and proof of consent.

In addition, and from an industry perspective, IAB Europe's TCF Policies also provides some general recommendations for the

establishment of roles and responsibilities of digital advertising actors. In particular, the Policies provides that vendors, i.e. companies that participates in the delivery of digital advertising within a publisher's website, app, or other digital content, may be considered under the GDPR as controllers, processors, or both, depending on the specific circumstances of the case.

In relation to the same, IAB Europe's Mobile In-App CMP API v1.0: Transparency & Consent Framework, which represents a specification dependent on the TCF dedicated to global interfaces within the mobile ecosystem of an app, also provides for an indication of vendors roles and responsibilities. Specifically, when vendors, among other actions, collects or receives personal data about the publisher's end users, they don't necessarily need to assume the role of controllers.

In practice, the following general recommendations can be considered when assigning roles and responsibilities to ad tech actors, always taking into consideration that roles under the GDPR cannot be assigned a priori, but must always follow a case by case assessment, also considering that a single subject may adopt more than one role.

- The publisher, who sell space on its website for the placement of targeted advertising, as well as the advertiser, will likely assume the role of controllers, as outlined above.
- Ad networks will likely assume the role of controllers, as outlined above.
- DMPs, used by publishers to examine data they retain in relation to their potential and current clients, may assume both the role of controller and processor, depending on the circumstances. For example, it will have to be considered in concrete whether the DMP provides itself data coming from third parties or limits itself to facilitating the acquisition of third-party data.

- CMPs, used by publishers to manage users' consent and marketing preferences, will in principle assume the role of processor. However, a case by case approach must be adopted in relation to the processing activities carried out by the CMP.

Are explicit consent and other derogations under Article 49 of the GDPR a viable option for the transfer of personal data collected and processed via third-party analytic and other kind of cookies following Schrems II?

The highly anticipated Schrems II judgment, as issued by the Court of Justice of the European Union (CJEU) on 16 July 2020, in Data Protection Commissioner v. Facebook Ireland Limited, Maximillian Schrems (C-311/18) declared, on the one hand, the EU-US Privacy Shield invalid, and, on the other, upheld the use of Standard Contractual Clauses ('SCCs'), providing clarity around the considerations that organizations and authorities should bear in mind if utilized as the transfer mechanism of choice.

When considering the use of cookies and other tracking technologies, organizations often use third party analytic cookies, as well as other kind of third-party cookies, for the purpose of monitoring the users' usage of a website/app. Since the third-party setting cookies may be based in a third country, the use of cookies may imply the collection and subsequent international transfer of personal data. As a result of the Schrems II judgment, organizations are required carry out an assessment of the possible transfer of personal data, in order to see whether the same can be deemed compliant with the judgment of the CJEU.

Organizations have been looking for viable solutions to transfer personal data to third countries post Schrems II, and the possibility regarding the derogations provided by Article 49 of the GDPR has been discussed, which can be implemented when:

- The third country does not provide adequate protection.
- No adequate safeguards aimed at providing protection for the data are being implemented.

Having said this, it is important to assess if the derogations can, in fact, be relied upon.

Explicit consent (Article 49(1)(a) of the GDPR)

The EDPB clarified in its latest FAQs on Schrems II that the transfer of personal data on the basis of explicit consent is allowed when the same consent is:

- Explicit.
- Specific for the particular data transfer or set of transfers, meaning that the data exporter must make sure to obtain specific consent before the transfer is put in place, even if this occurs after the collection of the data.
- Informed, with specific reference to the possible risks of the transfer. The data subjects should therefore be informed of the specific risks resulting from the fact that their data will be transferred to a country that does not provide adequate protection and that no adequate safeguards aimed at providing protection for the data are being implemented.

However, the EDPB stressed the fact that explicit consent, as the other derogations under Article 49 of the GDPR, are subject to a narrow interpretation, and must be considered as exceptions, and not as standard rules.

In relation to explicit consent, the Baden-Württemberg data protection authority also issued an orientation guide on the Schrems II case, outlining derogations under Article 49 of the GDPR as one possible transfer mechanism, but also recalling the narrow interpretation of the scope of Article 49 by the EDPB within its Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679 and stressing the fact that an exception

should not become the rule.

In practice, this derogation may find an application in relation to the transfer of personal data through cookies, given that certain cookies could be set on the basis of consent that re-collected only after a relevant amount of time (for example 6 months or 1 year).

Transfer necessary for the performance of a contract (Article 49(1)(b) of the GDPR)

The EDPB highlights in its FAQs on Schrems II that, in relation to transfers that are necessary for the performance of a contract between the data subject and the controller, organizations should take into consideration that this derogation can find application only when:

- the transfer is occasional (to be established on a case-by-case basis).
- the transfer is objectively necessary for the performance of the contract.

However, given the occasional nature of the transfer, it might be challenging to find an application of the above derogation to a transfer of personal data carried out through the setting of cookies.

Lastly, it must be recalled that the EDPB released, following the Schrems II judgment, on 11 November 2020, its Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data organizations and Recommendations 02/2020 on the European Essential Guarantees for surveillance measures.

The Recommendations 01/2020 aim to assist controllers as well as processors acting as data exporters with their duty to identify and implement appropriate supplementary measures where the same are needed to ensure an essentially equivalent level of protection data they transfer to third countries.

On the other hand, the Recommendations 02/2020, which constitute an updated version of the ones issued following the Schrems I Case invalidating Safe Harbor, aim to provide guidance on the elements to examine whether surveillance measures allowing access to personal data by either national security agencies or law enforcement authorities in a third country can be regarded as a justifiable interference or not.

Although the above recommendations do not directly address the transfer of personal data carried out through the use of cookies, organizations will have to take them into account when assessing their international data transfer activities.

Why did the French Conseil d'Etat rule against CNIL'S position on Cookie walls?

On 19 June, 2020 the Conseil d'Etat – which is the highest administrative court in France – issued decision No. 434684 that ruled on CNIL's powers to issue guidelines for compliance with data protection legislation, validating CNIL's guidelines in general and, overruling CNIL's position on cookie walls. The Conseil d'Etat did not rule over the substance of CNIL's position on cookie walls, it ruled over CNIL's capacity to issue such general and prohibitive policies.

The Guidelines issued by CNIL (délibération n° 2019-093 du 4 juillet 2019 de la Commission nationale de l'informatique et des libertés [CNIL] portant adoption de lignes directrices relatives à l'application de l'article 82 de la loi du 6 janvier 1978 modifiée aux opérations de lecture et écriture dans le terminal d'un utilisateur [notamment aux cookies et autres traceurs]) were challenged by a consortium of professional associations and unions in the e-commerce sector (i.e. l'association des agences-conseils en communication, la fédération du e-commerce et de la vente à

distance, le groupement des éditeurs de contenus et services en ligne, l'Interactive Advertising Bureau France, la Mobile Marketing Association France, le syndicat national communication directe de la data à la logistique, le syndicat des régies internet, l'union des entreprises de conseil et d'achat media et l'union des marques). These organisations filed a summary request at the litigation secretariat of the Conseil d'Etat requesting the invalidation of the CNIL Guidelines. The request for invalidation was sustained on the grounds of excessive power on the part of CNIL issuing obligations that lie beyond their realm of competence.

In their request, the consortium posed several questions challenging the power of CNIL and the current interpretation of article 2(f) of the ePrivacy Directive when read in light of Articles 4(11) and 95 of the GDPR (e.g.). The main challenge in the request was whether offers and contracts relating to access to digital content and services, under which the consumer undertakes to provide personal data to the professional are to be prohibited? The claimants went on to ask if, in case of a negative answer, should the aforementioned provisions be interpreted as banning CNIL from establishing a general prohibition offers and contracts relating to access to digital content and services where the exchange of personal data is required? Quite a binary approach from the claimants.

The formulation of the request was longer and included a sub-set of questions circling around the above two points, as well as more specific challenges relating to the use of tracking technologies and the limits of the consenting requirements established by CNIL. The request stressed on the applicable provisions that limit the use of "cookie walls", which - they claimed - in and of itself, unduly undermines the right to freedom of information as well the freedom to conduct business.

In its decision No. 434684, the Conseil d'Etat mandated the deletion of paragraph 4 in Article 2 of CNIL's recommendations prohibiting the use of Cookie Walls. The Conseil d'Etat ruled that the interpretation by CNIL of the requirements laid down in Article 4(11) GDPR was relying on a general and absolute prohibition inferred from the sole concept of "freely given consent". As a result the Conseil d'Etat overruled CNIL's powers on the general and absolute prohibition to rely on cookie walls.

Resources

Legislation

GDPR

https://eur-lex.europa.eu/eli/reg/2016/679/oj

ePrivacy Directive

https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX%3A02002L0058-20091219&from=EN

draft ePrivacy Regulation

https://eur-lex.europa.eu/legal-content/EN TXT/?uri=celex:52017PC0010

CCPA

https://leginfo.legislature.ca.gov/faces/codes_displayText.

Guidance

EU

European Commission:

cookie dedicated page

https://wikis.ec.europa.eu/display/WEBGUIDE/04.+Cookies

Draft ePrivacy Regulation explanatory memorandum

https://ec.europa.eu/digital-single-market/en/proposal-eprivacy-regulation

EDPS

Opinion No. 6/2017 on the ePrivacy Regulation

https://edps.europa.eu/sites/edp/files/publication/17-04-24_eprivacy_en.pdf

Article 29 Working Party
Opinion No. 3/2016 on the evaluation and review of the ePrivacy Directive

https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2016/wp240_en.pdf

EDPB
Guidelines 05/2020 on Consent under Regulation 2016/679

https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf

Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR

https://edpb.europa.eu/sites/edpb/files/files/file1/201905_edpb_opinion_eprivacydir_gdpr_interplay_en_0.pdf

ICO
Guidance on the use of cookies and similar technologies

https://ico.org.uk/for-organisations/guide-to-pecr/guidance-on-the-use-of-cookies-and-similar-technologies/

CNIL
Guidance on cookies and online trackers

https://nam01.safelinks.protection.outlook.com/GetUrlReputation

DSK
Guidance on telemedia providers

https://www.datenschutzkonferenz-online.de/media/oh/20190405_oh_tmg.pdf

AEPD
Guide on the use of cookies

https://www.aepd.es/sites/default/files/2019-12/guia-cookies-en_0.pdf

DPC
Guidance note on cookies and other tracking technologies

https://www.dataprotection.ie/sites/default/files/uploads/2020-04/Guidance%20note%20on%20cookies%20and%20other%20tracking%20technologies.pdf

IAB Europe
Transparency and Consent Framework ('TCF')

https://iabeurope.eu/transparency-consent-framework/

Case Law

Court of Justice of the European Union
Planet49 Case:

http://curia.europa.eu/juris/document/document.jsf?text=&docid=218462&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=4435561

Fashion ID Case:

http://curia.europa.eu/juris/document/document.jsf?text=&docid=216555&pageIndex=0&doclang=en&mode=req&dir=&occ=first&part=1&cid=4868067

OneTrust
How OneTrust Helps: CCPA "Do Not Sell" Requirements

https://www.onetrust.com/how-onetrust-helps-ccpa-do-not-sell-requirmements/

OneTrust Consent Management Platform is IAB TCF 2.0 Approved CMP

https://www.onetrust.com/onetrust-consent-management-platform-is-iab-tcf-2-0-approved/

OneTrust

PRIVACY, SECURITY & GOVERNANCE

DEFINING THE FUTURE OF PRIVACY, SECURITY & GOVERNANCE

Powered by 130 awarded patents, our platform drives innovative compliance programs for companies of all sizes across the globe

TECHNOLOGY PLATFORM

Most depth and breadth of privacy & security use cases than any solution in the market

REGULATORY RESEARCH

Most intelligent platform powered by massive regulatory datasets updated daily

PROFESSIONAL SERVICES

Most certified resources available worldwide to support your deployment

USER COMMUNITY

Largest and most active global community sharing best practices

ONLINE DEMO | ONETRUST.COM

OneTrust

PRIVACY, SECURITY & GOVERNANCE

INQUIRIES

info@onetrust.com

SUPPORT

support@onetrust.com

WEB

www.onetrust.com

LOCATIONS

Atlanta | London | Bangalore | Melbourne
Seattle | San Francisco | New York | São Paulo
Munich | Paris | Hong Kong | Bangkok