RPIN

PIN CODE

REVUE INTERNATIONALE DE LA PROPRIÉTÉ INTELLECTUELLE ET DU DROIT DU NUMÉRIQUE

#13 **ISSN** 2658-9869
JANVIER 2023

LEGI TECH éditeur juridique

Doctrine

COOKIES REGULATIONS: AN INTERNATIONAL OUTLOOK

INTRODUCTION, EU AND LUXEMBOURG – COORDINATION

GARY CYWIE
PARTNER

Canada
CHARLES MORGAN
PARTNER
cmorgan@mccarthy.ca

France
FABRICE PERBOST
PARTNER
fperbost@harlaylaw.com

Germany
ALEXANDER BRANDT
SENIOR ASSOCIATE
alexander.brandt@noerr.com

Hong Kong
PADRAIG WALSH
PARTNER
padraigwalsh@tannerdewitt.com

Mainland China
JUN YANG
PARTNER
jun.yang@jadefountain.com

United Kingdom
EDUARDO USTARAN
PARTNER
eduardo.ustaran@hoganlovells.com

In computer science, a cookie is a file with an embedded message. In practice, it is simply a small text file that travels from a web browser or application on a computer or mobile device to a web server.

Cookies can be used to track web and app activities and keep browsing histories: they can store unique identifiers to recognize a visitor and record which type of device and browser they use, which webpage they are coming from, what they look for, how much time they stay on a webpage, where they click, etc. This can benefit the visitor and websites get a lot out of it as well. There exist other technologies similar to cookies such as device fingerprints, pixels, web beacons and shared objects. Depending on the relevant circumstances, the same regime may apply to those technologies.

Cookies can be set by the websites you visit and the information stored in the cookies be automatically sent back upon each of your further interactions with these websites. Websites can also use external services which can set their own cookies, known as third-party cookies.

From a technical perspective, there are mainly two types of cookies: session cookies are only used during the time one navigates a specific website – they are deleted at the end of the session, when the user disconnects or closes all the pages of the website – whereas to the contrary persistent cookies remain on the computer for a long period, sometimes months if not years. Cookies may have different functions and can be used for various purposes. Some cookies are not very intrusive but others may have more implications in terms of privacy as they are aiming at tracking, profiling and targeting users.

The internet being itself borderless and the services of many websites being proposed in various countries, we thought it would be interesting to have a closer look at how cookies and similar technologies are regulated in some different jurisdictions in the European Union and around the world, especially as they may have an extraterritorial reach. Other legislation such as the California Consumer Privacy Act or the Brazilian Lei Geral de Proteção de Dados Pessoais *could be tackled in a next edition.*

This article focuses on regulations specifically governing cookies and similar technologies and does not purport to provide an overview of any and all rules applicable to them, notably in relation to transfers of personal data from EU Member States to third countries, for example, that may result from the use of certain cookies.

I. IN THE EUROPEAN UNION

A. European Union regulation

1) General principle: prior consent necessary to store or access information in cookies

Cookies are mainly regulated by the e-Privacy Directive[1] and its implementation legislation in EU Member States and the GDPR.[2]

In accordance with Article 5(3)[3] of the e-Privacy Directive, storing information, or accessing information already stored, in users' or subscribers' terminal equipment such as computers or smartphones – which is in a technology neutral language what cookies do – require by way of general principle the prior consent of the user or subscriber concerned, the so-called "cookie consent".

When looking at cookies from a data protection standpoint, i.e. at least when information stored or accessed in cookies qualify as personal data (which would most of the time be the case), the GDPR must be considered. Following a request from the Belgian data protection authority, on 12 March 2019 the EDPB[4] adopted its Opinion 5/2019 on the interplay between the e-Privacy Directive and the GDPR. That Opinion recalls that certain processing activities may fall within the material scope of application of both the e-Privacy Directive and the GDPR. The EDPB nevertheless emphasises that, in accordance with the adage *lex specialis derogat legi generali*, the general rules set out in the GDPR shall apply in the absence of specific provisions governing a particular processing operation or set of operations, in particular in relation to the rights granted to data subjects.

Besides, in any case where Article 5(3) of the e-Privacy Directive requires consent to be obtained, such consent needs to comply with the requirements of the GDPR.[5] Under Article 4 of the GDPR, consent is defined as a "freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her". Cookie consent must therefore follow that definition and, in particular, follow the requirements of informed consent set out in the GDPR.

Accordingly, it is also important to avoid serving cookies requiring consent before having obtained the consent, and the absence of "clear affirmative action" should always be interpreted as the absence of consent. For example, simply continuing to visit a website does generally not imply consent, even if a cookie banner says so. In addition, consent may have to be renewed after a certain period, to be determined in accordance with the specific circumstances at hand.

In *Planet49*, a quite important decision in relation to the use of cookies and the internet in general seen from a European Union perspective at least, the CJEU[6] clarified that Article 5(3) equally applies regardless of whether or not the information stored or accessed through the cookies concerned qualify as personal data within the meaning of the GDPR.[7]

In that ruling, the CJEU concludes that storing cookies requires the users' active consent. A pre-ticked checkbox is therefore insufficient.

Detailed guidance about the use of cookies can alsobe found in the 29 Working Party Opinion 2/2010 on online behavioural advertising and Opinion 16/2011 on the EASA/IAB Best Practice Recommendation on Online Behavioural Advertising as well as EDPB Guidelines 05/2020 on consent under the GDPR and Guidelines 3/2022 on Dark patterns in social media platform interfaces: How to recognise and avoid them.

2) Exception: consent exemption for "strictly necessary" cookies

As outlined in Opinion 04/2012 on Cookie Consent Exemption adopted on 7 June 2012 by the 29 Working Party,[8] Article 5(3) of the e-Privacy Directive provides for two exemptions to the informed consent requirement.[9]

1. Directive 2002/58 of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the communications sector, as amended by Directive 2009/136/EC.
2. General Data Protection Regulation (Regulation EU 2016/679).
3. "Member States shall ensure that the storing of information, or the gaining of access to information already stored, in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned has given his or her consent, having been provided with clear and comprehensive information, in accordance with Directive 95/46/EC, inter alia, about the purposes of the processing."
4. European Data Protection Board. The EDPB is an independent European body, which contributes to the consistent application of data protection rules throughout the European Union, composed of notably representatives of the EU national data protection authorities.
5. For the definition of consent, Article 2(f) of the e-Privacy Directive refers to Directive 95/46/EC, the former data protection directive that was repealed by the GDPR. By application of the first sentence of Article 94(2) of the GDPR, such reference now needs to be read as made to the GDPR.
6. Court of Justice of the European Union. The CJEU is the judicial authority of the European Union ensuring the uniform application and interpretation of EU law.
7. CJEU, Planet49 GmbH v. Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband e.V. (*Planet49*), C-673/17, pt. 71.
8. The 29 Working Party is the predecessor of the EDPB under the EU data protection directive that was repealed by the GDPR.
9. "This shall not prevent any technical storage or access for the sole purpose of carrying out the transmission of a communication over an electronic communications network, or as strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service."

The first exception concerns cookies used "for the sole purpose of carrying out the transmission of a communication over an electronic communications network" (*emphasis added*). As stressed under the Opinion mentioned above, this criterion does not leave much room for interpretation: "Simply using a cookie to assist, speed up or regulate the transmission of a communication over an electronic communications network is not sufficient. The transmission of the communication must not be possible without the use of the cookie."

The second exception concerns storage or technical access "strictly necessary for the provider to provide an information society service expressly requested by the subscriber or user" (*emphasis added*).

The "strictly necessary" exemption requires that storing the information (or accessing it) must be essential, rather than important or simply necessary to provide the service requested by the user (including in terms of security, for example, as required under the GDPR). Put simply: "if cookies are disabled, the service will not work", as stated in the Opinion mentioned above. Otherwise, the consent of users is required.

What is "strictly necessary" should be assessed from atechnical perspective and from the perspective of the user or subscriber rather than from the perspective of the website provider's economical interest. So advertising cookies that generate revenue that funds a provider's service are not "strictly necessary" from the user's or subscriber's perspective.

Even if one of the consent exemptions applies, information must still be provided to the user or subscriber as per Articles 12 to 14 of the GDPR when the use of cookies involves the processing of personal data.

Cookies likely to be considered strictly necessary include those allowing the website to remember the goods a user wishes to purchase when they check out or add goods to their shopping basket, to comply with the security principle for an activity that the user has requested, for example in relation to online banking, session cookies that are only used to remember a user's authentication during their visit on a website and cookies whose sole purpose is the identification of the communication endpoints for load balancing purposes.

Cookies unlikely to be considered as strictly necessary include, for example, those used for analytical purposes, e.g. to count the number of unique visits to a website; first-party and third-party advertising cookies, including those used for operational purposes related to third-party advertising, such as click fraud detection, research, product improvement, etc. or cookies used to recognise a returning visitor, e.g. to adapt a welcome message.

It is also interesting to note that the Opinion mentioned above states that "a cookie that is exempted from consent should have a lifespan that is in direct relation to the purpose it is used for, and must be set to expire when it is no longer needed, taking into account the reasonable expectations of the average user or subscriber. This suggests that cookies that match [the cookie consent exemptions] will likely be cookies that are set to expire when the browser session ends or even earlier."

3) Consent exemption does not relieve from providing the necessary information

Importantly enough, none of the consent exemption exempts the service provider from providing the necessary information to the users as per Articles 12 to 14 of the GDPR when the use of cookies involves the processing of personal data. According to the GDPR, the information must notably be provided in a concise, transparent, intelligible, easily accessible fashion by using clear and plain language.

In *Planet49*,[10] the CJEU also ruled that Article 5(3) of the e-Privacy Directive must be interpreted as meaning that the information that the service provider must give to website users include the duration of the operation of cookies and whether or not third parties may have access to those cookies, in addition to the purposes explicitly referred to in Article 5(3).

4) Further harmonisation in the European Union with the proposed e-Privacy Regulation?

Finally, the (forthcoming?) adoption of the European Commission proposal for an e-Privacy Regulation[11] should further harmonise the rules governing the use of cookies at least within the European Union and, at the same time, bring more legal security and potentially also further possibilities to service providers, such as other consent exemptions.

That proposal was adopted on 10 January 2017, with the aim of replacing the current legal framework of the e-Privacy Directive. On 10 February 2021, the Council of the Eu-

10. CJEU, *ibid.*, pt. 81.

11. Proposal for a regulation on the respect for private life and the protection of personal data in electronic communications.

ropean Union published a press release according to which the EU Member States' representatives at the Council (Committee of Permanent Representatives or "Coreper") agreed to grant a negotiating mandate to the Council for the revised rules on the protection of privacy and confidentiality in the use of electronic communications services.[12]

Hence, after years of a certain legislative slowdown, such a mandate of negotiation may finally permit the launch of a "*trilogue*" legislative process (between the Parliament, the Council and the Commission) with a view to reaching a final agreement on the content on the said e-Privacy Regulation (not expected any time soon though).

The e-Privacy Regulation may, for example, provide additional guidance on cookie walls.[13] Recital 18 of that proposal says that "Consent for processing data from internet or voice communication usage will not be valid if the data subject has no genuine and free choice, or is unable to refuse or withdraw consent without detriment." Therefore, making access to a website dependent on consent to the use of cookies for additional purposes would in principle not be possible, except in certain specific circumstances that should be further specified. A true alternative without cookies should be available, as otherwise consent would not be freely given, as per the requirement for valid consent under the GDPR. However, the new e-Privacy Regulation may include new consent exemptions allowing website providers to use, for example, audience measuring solutions without consent.

B. France

The provisions on cookies set in the e-Privacy Directive were transposed into French national law under Article 82 of the French Data Protection Act No. 78-17 of 6 January 1978 as amended which also governs the processing of personal data.

The French Data Protection Authority ("CNIL") is empowered to ensure compliance and to sanction any breach of the French Data Protection Act, including use of cookies regardless of the kind of data (personal data or not) stored or accessed through cookies.

To provide guidance on cookies and the interplay with the GDPR, the CNIL issued on 17 September 2020 two sets of soft-law documents: guidelines and recommendation on cookies. The guidelines aim at explaining the legal framework applicable to cookies while the recommendation provides practical examples for obtaining consent. An FAQ on common questions raised by the guidelines or the recommendation was also published and is beingupdated regularly. The main focus of those documents is the conditions to collect and demonstrate having valid consent.

Firstly, merely browsing a website or scrolling a webpage is no longer considered as valid consent to cookies and is equally considered the absence of any positive action by users such as merely closing the consent manager tool. Secondly, the CNIL suggests using a two-layer information to provide the relevant information to data subject prior to accepting or refusing cookies and calls for website operators to pay careful attention on the consent tool to avoid any dark pattern that would be misleading. Thirdly, withdrawing from consent or refusing cookies should be as easy as providing consent, so acceptance and refusal buttons must be displayed on the same page and access to a consent management tool shall be available on every webpage. Fourthly, users shall be provided with an up-to-date list of all cookie's operators involved as data controllers when setting a cookie. Finally, as such cookie operators must be able to provide, at any time, proof of the valid consent, the CNIL issued practical recommendation on means to use to provide evidence like source code escrow of the consent management tool, screenshot with a timestamp of the consent page, regular audit of tools used, information and documentation of third party consent management platforms ("CMP") that the website operator relies on.

Based on its knowledge and the actual state-of-the art, the data privacy authority issued a non-exhaustive list of cookies falling within the "strictly necessary" exemption which includes cookies used to store consent, authentication cookies (including those for security to limit robotic or unexpected access attempts), cookies to remember the shopping basket, cookies for personalizing the user interface (e.g. for language or presentation preference), load balancing cookies, analytics cookies under strict conditions and cashback/reward cookies.

The French authority further considers that analytics cookies may be exempted (as a strictly necessarycookies) provided that the four following criteria are met in relation to these cookies: (i) are strictly limited to the sole purpose of measuring the audience on the website/app for the exclusive benefit of the website/app operator; (ii) is only used to produce anonymous statistical data; (iii) no global tracking of users occurs when they navigate on other applications or websites; and (iv) data is not reconciled with other processing or passed on to third parties.[14]

12. See https://www.consilium.europa.eu/en/press/press-releases/2021/02/10/confidentiality-of-electronic-communications-council-agrees-its-position-on-eprivacy-rules/.

13. This topic was covered in the previous edition of PIN CODE.

14. Please see likely different interpretation in Germany under section C below, ninth paragraph.

With respect to cashback / reward cookies, the French Supreme Court (*Conseil d'État*) confirmed that those cookies may be considered as strictly necessary when users contract to subscribe to such services.

Furthermore, it should be noted that the CNIL made suggestions relating to the lifespan of certain cookies: cookies used to retain the choice over the use of cookies (consent or refusal) should be limited to six months while analytical cookies should not be stored for a period exceeding thirteen months.

Finally, on the practice of cookies walls, the CNIL initially held a firm prohibition position which was overturned by a ruling of the French Supreme Court. The position of the data protection authority was then fine-tuned and resulted in guidelines published in June 2022, which provided a set of criteria to assess the legality of the cookie wall. The CNIL still considers that use of a cookie wall is likely to infringe, in certain cases, the freedom of choice of the users and thus recommends following a case-by-case reasoning taking into consideration, in particular, the existence of real and fair alternative(s) for users. If, for instance, a content is available for free while agreeing to cookies or upon payment of a fee without cookies, then the fee has to be reasonable otherwise it would deprive the user of a genuine choice.

Compliance on the use of cookies was on the CNIL's agenda for priority controls in 2021 and 2022. In January 2022, the CNIL announced that it had already adopted almost 100 corrective measures (formal notices and administrative fines) since 31 March 2021, in relation to non-compliant use of cookies.

C. Germany

Article 5(3) of the e-Privacy Directive was only recently (as of 1 December 2021; and, thus, much too late) transposed into German national law formally and properly. Section 25 of the German Telecommunication-Telemedia-Data Protection-Law (TTDSG[15] transposes Article 5(3) of thee-Privacy Directive into national law, essentially word-by-word. Earlier legislative intentions to stipulate deviations from Article 5(3) of the e-Privacy Directive (which would have anyway been critical in terms of conformity with EU law) were dropped in the legislative process.

At least until the TTDSG came into force, there was high legal uncertainty as to the requirements on cookies and similar technologies in Germany, especially since the predecessor of Section 25 of the TTDSG, Section 15(3) of the former version of the German Telemedia Act, essentially stipulated the opposite of what Article 5(3) of the e-Privacy Directive requires (i.e. the former German law, at least in its wording, generally required an opt-out-solution as opposed to opt-in). Only shortly before the TTDSG came into force, the German Federal Court of Justice somewhat clarified the legal situation by interpreting (contrary to previous guidance of data protection authorities) Section 15(3) of the former version of the German Telemedia Act in the light of Article 5(3) of the e-Privacy Directive.[16]

The German Data Protection Conference (*Datenschutzkonferenz*; "**DSK**" – the joint committee of the independent German data protection supervisory authorities at federal and state level) published on 20 December 2021 their updated guidance on telemedia in which the DSK discusses essential issues under Section 25 of the TTDSG.[17]

The DSK's guidance includes an analysis of Section 25 of the TTDSG and also discusses essential requirements on the processing of personal data under the GDPR in the context of telemedia and the use of cookies and similar technologies. The authorities recall that, most of the time, the use of cookies or similar technologies goes along with the processing of personal data and that the e-Privacy Directive, in the form of its implementation in Section 25 of the TTDSG, only precedes[18] the GDPR to the extent it stipulates specific requirements on the use of such technologies. Thus, any processing of personal data other than the mere access to information already stored on a device or the mere storage of information on a device is fully subject to the GDPR.

From a practical perspective, the DSK guidance shows that it is important to consider data protection law also in the wording of a consent banner. For example, where the processing of personal data in the context of cookies is supposed to be based on consent within the meaning of Article 6(1)(a) GDPR (in addition to consent under Section 25 of the TTDSG), the consent banner needs to be clear on this and, especially, must not be limited to explaining the mere use of cookies but needs to cover also the subsequent processing activities that are supposed to be based on consent. It is therefore advisable to design such consent banners not as mere "cookie banners" but to understand, and potentially even label, them as "data protection and cookie settings".

15. Telekommunikation-Telemedien-Datenschutz-Gesetz, see https://www.gesetze-im-internet.de/ttdsg/__25.html.
16. See German Federal Court of Justice (BGH), ruling of 28.05.2020, case reference I ZR 7/16.
17. See DSK, Orientierungshilfe der Aufsichtsbehörden für Anbieter:innen von Telemedien ab dem 1. Dezember 2021, in the updated version 1.1 as of 5 December 2022, available (only in German) under https://www.datenschutzkonferenz-online.de/media/oh/20221205_oh_Telemedien_2021_Version_1_1_Vorlage_104_DSK_final.pdf.
18. Subject to Article 95 of the GDPR.

In German legal literature, the scope of Section 25 of the TTDSG (and Article 5(3) of the of the e-Privacy Directive) is disputed. While it is clear that the provisions apply to cookies and Local Storage-/Session Storage-Objects, it is disputed whether they also apply to browser fingerprinting or pixels/web beacons. Looking at the guidance of the DSK, it is well arguable that these provisions do not apply to such technologies in all cases even if they allow a certain tracking. The DSK describes the use of browser fingerprinting and, in this context, explains that Section 25 of the TTDSG (and Article 5(3) of the of the e-Privacy Directive) would not apply if only information was used for creating browser fingerprints that the browser automatically sends without being asked for, e.g. the IP address, the requested URL, the User-Agent-String with information on the version of the browser and the operating system and the language set in the browser (essentially the data that is sent automatically with each HTTP request). The reasoning behind this is that this is not "storing of information" on the device and also not "gaining access to information already stored" because the device shares this information automatically and it is not actively accessed by the website provider. Contrarily, in the view of the DSK, browser fingerprinting would be subject to Section 25 of the TTDSG (and Article 5(3) of the of the e-Privacy Directive) if the fingerprints were based on information that is actively retrieved by the website provider from the device, e.g. by using JavaScript codes that assist in reading out and sending to the server information on the device's settings and properties.

For cases where consent is required under Section 25 of the TTDSG (and Article 5(3) of the of the e-Privacy Directive), the DSK reiterates in their guidance that such consent needs to be given on an "informed" basis. In this context, it is of course necessary to transparently describe the activities that are supposed to be based on consent. However, the DSK also points out that it also needs to be transparent how and with which effort users can refuse to grant consent. The authorities also point out that the information on the website as a whole needs to be transparent and consistent, especially the information in a consent banner and in the data protection information (or privacy policy) need to be consistent. In practice, this often proves to be somewhat of a hurdle – especially if the consent banners are based on standardised consent solutions that base the information on standard text generated upon automatically crawling the website for cookies and similar technologies (as opposed to manually describing the relevant tools and technologies, both in the consent banner and in the data protection information).

As for exemptions of the consent requirements under Section 25 of the TTDSG (and Article 5(3) of the of the e-Privacy Directive), the guidance remains rather careful/vague and provides general guidance on how to assess whether exemptions apply rather than specific examples where such examples do or do not apply. For example, there is no clear indication on whether web analysis, A/B testing, audience measuring etc. can be subject to such exemptions, so that there at least remains some room to argue. However, looking at the general guidance, the wording of Section 25 of the TTDSG (and Article 5(3) of the of the e-Privacy Directive) and other statements of German data protection authorities,[19] there is a rather high likelihood that an authority would typically (but still subject to a case-by-case assessment) consider the use of such technologies not to be strictly necessary so that consent would be required.[20]

Noteworthy, at least in their updated Version 1.1 of 5 December 2022, the DSK now outlines that audience measuring may, subject to a case-by-case assessment, be permissible without consent if it is done only for the purpose of the error-free provision of the website (and not, for example, also for measuring the economic efficiency of advertisements).

As for cookies or similar technologies that may definitely be strictly necessary in the relevant cases (e.g. shopping cart cookies), the authorities point out that such cookies are only exempt from the consent requirement to the extent this is actually necessary. For example, (1) a shopping cart cookie would typically not be necessary while the user is merely browsing an online store but only upon putting the first item into the shopping cart or (2) a language selection cookie would typically not require storing a unique user ID in a cookie but it would generally be sufficient to store only the selected language identifier.

In practice, it is therefore essential to consider these requirements early in the process of designing a website and to ensure compliance by establishing relevant guidance for internal programmers, external agencies etc. – such internal guidance should of course also cover other related topics which may not be subject to Section 25 of the TTDSG (and Article 5(3) of the of the e-Privacy Directive) but which are likewise important, e.g. the issues on implementing external resources, such as fonts, script libraries, maps, video players, etc.

19. For example, the supervisory authority of Baden-Württemberg (*Der Landesbauftragte für Datenschutz und Informationsfreiheit Baden-Württemberg*) very clearly states that web audience measuring on the basis of cookies or similar technologies requires consent, see. https://www.baden-wuerttemberg.datenschutz.de/faq-zu-cookies-und-tracking-2/#31_darf_ich_werkzeuge_zur_reichweitenanalyse_ohne_einwilligung_der_nutzendenverwenden.

20. Please see different interpretation in France under section B below, seventh paragraph.

D. Luxembourg

The e-Privacy Directive was transposed into Luxembourg law by the Luxembourg e-Privacy Law, amended several times since then.[21]

Article 4 relating to the confidentiality of communications provides that "any service provider or operator guarantees the confidentiality of communications carried out by means of a network of public communications and electronic communications services available to the public, as well as the confidentiality of related traffic data."

According to the second paragraph of the same "it is forbidden for anyone other than the user concerned to listen to, intercept, store communications and related traffic data, or subject them to any other means of interception or surveillance without the consent of the user concerned."

Although these legal provisions seem to apply to network operators and electronic communications service providers only, the third paragraph, point (e) says that the second paragraph mentioned above "does not apply to storing information, or obtaining access to information already stored, in the terminal equipment of a subscriber or user provided that the subscriber or user has given his consent, after having received a clear and complete information, including on the purposes of the processing. The methods used to provide the information and offering the right of refusal should be as user-friendly as possible. When technically possible and effective, subscriber or user consent may be expressed through the use of appropriate browser or web browser settings."

Finally, it says "that provision does not impede technical storage or access aimed exclusively at carrying out the transmission of a communication byway of an electronic communications network, or strictly necessary for the provision of a service of the information society expressly requested by the subscriber or user."

Article 4 of the Luxembourg e-Privacy Law is criminally sanctioned, showing the importance given by the legislator to the matter. In practice, however, to the best of our knowledge, there has been no sentence in this respect since the adoption of the law.

On 26 October 2021, the national data protection authority, the CNPD[22] published updated Guidelines on cookies and similar tracking technologies.[23] These Guidelines provide an outlook of the European Union and national legal framework, including the principles that have been summarised above.[24] The Guidelines contains many practical tips as well as examples of good practices and behaviours that must be avoided. Consent gathering processes designed to influence or even mislead the choice of users are shown to exemplify such behaviours, including for example presenting the consent button in a bigger or stronger colour than the refusal button or even worse not presenting the refusal button at all.

In particular, the Guidelines provide practical examples in relation to each of the criteria required for obtaining valid consent, namely, informed, prior consent, freely given, unambiguous positive action, specific. Additionally, the CNPD recalls the principle according to which it should be possible to refuse or withdraw consent, the validity of the consent over time and the necessity to renew consent and how to prove the latter. Regarding the validity period of consent, the CNPD suggests as a general rule of thumb that it should be renewed after 12 months. It should be as easy to refuse consent as it is to give it. If one click is enough to consent, refusal should also be possible in one click.

We note in particular the necessity to provide means for users to return to the cookies management interface, for example by using a hyperlink located atthe bottom of each page of the website concerned or by using a floating button accessible at any time.

Finally, the CNPD recalls that when the use of cookies involves the processing of personal data, the GDPR will fully apply and, in particular, fully-fledged information in accordance with Article 13 thereof must be provided to users in relation to that processing.

II. OUTSIDE OF THE EUROPEAN UNION

A. Canada[25]

Unlike the European Union, Canada does not have any current legislation that specifically and narrowly applies to the regulation of "cookies". Instead, the Canadian approach to the regulation of "cookies" relies on a patchwork of privacy laws of general application. Primary among these are federal and provincial privacy laws such as the federal Personal Information Protection and Electronic Documents Act (PIPEDA)[26] and the Quebec *Act Respecting the Personal Information in the Private Sector*

21. Law of 30 May 2005 on the protection of privacy in the electronic communications sector.
22. *Commission Nationale pour la Protection des Données*. The CNPD is the Luxembourg data protection supervisory authority as per the GDPR.
23. CNPD, « *Lignes directrices en matière de cookies et autres traceurs* », 20/11/2021. See https://cnpd.public.lu/fr/dossiers-thematiques/cookies.html.
24. See I.A above.
25. The author wishes to acknowledge the assistance of Olga Abimana is the research and drafting of this chapter.
26. PIPEDA would be replaced by the *Consumer Privacy Protection Act* (CPPA) which is the first Act of *Bill C-11 – the Digital Charter Implementation Act*.

(the "Quebec Privacy Act")[27], which govern the collection, use and disclosure of personal information gathered by all means of collection, not merely personal information gathered by means of the use of cookies. In this context, it should be noted, at the outset, that to the extent that cookies are not used to collect personal information, they are not subject to regulation in Canada.

Under PIPEDA and substantially similar provincialprivacy legislation, "personal information" is broadly defined as "information about an identifiable individual." In its 2011 Guidelines on privacy and online behavioural advertising, the Office of the Privacy Commissioner of Canada, applying basic privacy principles under PIPEDA, stated that the "collection or use of an individual's web browsing activity"[28] using tracking and targeting technology such as cookies "must be done with that person's knowledge and consent"[29]. Similarly, in 2016, the *Commission d'accès à l'information du Québec* pointed out that companies using profiling and targeted advertising systems on the Internet fall under the Act Respecting the Personal Information in the Private Sector.[30] As a result of the requirements of these privacy laws of general application, most Canadian companies treat the collection of personal information using cookies as a standard disclosure feature of their online privacy policies. They do not typically resort to the use of website cookie "pop-up" consents.

However, standard practice regarding cookie consents may evolve as a result of recent legislative developments. Specifically, the Quebec government has adopted amendments to the Quebec Privacy Act in September 2021 (pursuant to Bill 64) that bring specific regulatory scrutiny to organizations that collect personal information using technologies with functions allowing the person concerned to be identified, located or profiled. The definition of "profiling" set out in clause 8.1 of Bill 64[31] is similar to the definition of "profiling" found in clause 4(4) of the GDPR.[32] Although Section 8.1 of the Quebec Privacy Act does not use the word "cookie", a preliminary reading of the provision would suggest that such "profiling" technologies could include "cookies".[33] This interpretation of Section 8.1 is currently uncertain, however, since a related provision of the Quebec Privacy Act, section 9.1 (which requires businesses to ensure that, by default, the parameters of their technological product or service provide the highest level of confidentiality without any intervention by the person concerned – in furtherance of the "privacy by design" principle) expressly does not apply to the privacy settings of a cookie.

Nevertheless, section 8.1 of the Quebec Privacy Act requires organizations to notify individuals before collecting personal data using technologies with identification, location, or profiling functions, as well as how to "activate" these functions. By implication (if not expressly), the section appears to require that such technologies must be deactivated by default. Accordingly, as of 22 September 2023, when these new requirements take effect, businesses that wish to use such technologies – even in situations where explicit consent is not required – must employ an express notification strategy (for instance, through a pop-up window) that alerts the person to the use of the technology and instructs them on how to activate it.

With respect to consent, Section 14 of the Quebec Privacy Act (as amended by Bill 64) requires a "clear, free, and informed", consent that "must be given for specific purposes". Subsequently, consent must be requested in "clear and simple language" for each purpose. Such consent is only valid "for the time necessary to achieve the purposes for which it was requested".[34] Although consents related to the collection of personal information that have been obtained prior to the coming into effect of Bill 64 will remain valid, to the extent that Bill 64 imposes new disclosure obligations (as is the case of technologies with profiling functions under Section 8.1), consent may be required to be updated or re-established. Finally, it should be noted that Section 14 of the Quebec Privacy Act (as amended by Bill 64) does not require express consent. The only time express consent is necessary is when dealing with sensitive personal information.[35]

B. Hong Kong[36]

The primary legislation in Hong Kong that regulates cookies is the Personal Data (Privacy) Ordinance ("PDPO").[37] Also, the Privacy Commissioner for Personal Data ("PCPD") has issued guidance notes that provide helpful

27. The Quebec's private Sector Privacy Act would be amended by *Bill 64 – An Act to modernize legislative provisions as regards the protection of personal information.*

28. Office of the privacy Commissioner of Canada, *Guidelines on privacy and online behavioural advertising* (Ottawa, 13 August 2021), see https://www.priv.gc.ca/en/privacy-topics/technology/online-privacy-tracking-cookies/tracking-and-ads/gl_ba_1112/

29. *Ibid.*

30. Québec, Commission d'accès à l'information du Québec, *Publicité ciblée et protection des renseignements personnels* (Montréal, 16 March 2016), see https://www.cai.gouv.qc.ca/publicite-ciblee-et-protection-des-renseignements-personnels/

31. "Profiling means the collection and use of personal information to assess certain characteristics of a natural person, in particular for the purpose of analyzing that person's work performance, economic situation, health, personal preferences, interests or behaviour". Bill 64, *An Act to modernize legislative provisions as regards the protection of personal information*, 1st Sess, 42nd Leg, Quebec, 2020, cl 8.1.

32. EC, *EU General Data Protection Regulation (GDPR):* Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, s 4, see https://gdpr.eu/article-4-definitions/. "profiling" means "any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements."

33. A plain reading of the Act suggests that cl 8.1 requires that cookies with identification, localization or profiling functions are deactivated by default (opt-in). For cookies without such functions, cl 8.1 does not apply and the cookies can be activated by default. *Supra* note 6.

34. *Ibid.*, cl 14(3).

35. *Ibid.*, cls 12(1) & 13(2).

36. With the participation of Tara Chan and Julian Chan.

37. (Cap. 486).

guidance to the public about personal data protection and use of cookies. PCPD guidance notes are not mandatory but are recommended practices for practitioners to follow.

1) Personal data in Hong Kong

The PDPO regulates how data users collect, process and use personal data.

A "data user", in relation to personal data, means a person who, either alone or jointly or in common with other persons, controls the collection, holding, processing or use of personal data. It is the term under Hong Kong law that most closely approximates to data controllers.

The PDPO defines "personal data" as any data that:
(a) relates directly or indirectly to a living individual;
(b) is practicable to ascertain the identity of the individual; and
(c) is in a form in which access to or processing of the data is practicable.

Not all cookies are considered as processing personal data. If a cookie contains data that can identify a person uniquely, then the cookie will be considered personal data. An example would be information containing a name or telephone number. However, ifthe cookie does not uniquely identify a person, then the cookie may not be considered personal data and may fall outside the scope of protection under the PDPO. For example, an IP address was held not to be personal data as it was information about an inanimate computer, not an individual. The username "huoyan_1989" for a free email service provider was also not considered personal data as it was insufficient to ascertain the user's identity. These are interesting points of contrast to the position in the European Economic Area under the General Data Protection Regulation, where a different definition of personal data is used and email addresses and IP addresses would likely be considered personal data.

2) Are consent statements required?

Hong Kong follows a practice of informed but implied consent upon collection of personal data, except if direct marketing is intended. This practice must be followed for cookies processing personal data.

On or before collection of the personal data of a data subject, a data user must inform the data subject of:
(a) the personal data that will be collected;
(b) the purposes for which the personal data will be used;
(c) the classes of transferees to which the personal data may be transferred or shared;
(d) whether it is obligatory or voluntary for the data subject to supply his personal data;
(e) whether the personal data will be used for direct marketing; and
(f) his right to access and correct his personal data and the contact details to do so.

These obligations are met by providing the data subject a personal information collection statement on or before collection of the personal data. Once this requirement is fulfilled, then express or written consent of the data subject is only required if the data user changes the purposes for which the personal data may be used (including the classes of transferees). The position is different if cookies contain personal data and their use will be for direct marketing purposes. In this situation, the express, voluntary, specific and separate consent of the data subject must be obtained on or before collection of the personal data by the relevant cookie.

3) What should data users do?

The PCPD has issued guidance notes that apply to cookies and provide information, recommendations and practices that data users should adopt. These recommendations include:
(a) website owners should explicitly state what kind of information is stored in the cookies, regardless of whether personal data is involved.
(b) pre-set a reasonable expiry date for cookies.
(c) encrypt the contents of cookies whenever appropriate.
(d) do not deploy techniques such as super cookies that ignore browser settings on cookies unless the website owner can offer an option to disable or reject the use of such cookies.
(e) inform website users about the purpose of collecting the information and obtain express and voluntary consent for any change to the purpose of use.
(f) take steps to protect the collected information from unauthorised access, disclosure or loss.
(g) if third-party cookies are deployed, the website owner should also clearly state the type of information collected and to whom such information may be transferred to.
(h) if the acceptance of the use of cookies is mandatory, then this requirement should be clearly stated on the website.
(i) if acceptance of use of cookies is voluntary, the website should provide users with an option to accept or decline the use of cookies, and clear information of the consequences if users decline the use of cookies (for example loss of certain functionality).

C. Mainland China[38]

The use of cookies and similar tracking technologies in the People's Republic of China is essentially governed by the PRC Personal Information Protection Law of 20 August 2021 ("PIPL", which took effect on 1st November 2021) and other associated national standards.

Personal information is defined under Article 4 of the PIPL as "*information relating to an identified or identifiable individual recorded by electronic or other means*" (*emphasis added*). Appendix A of the Information security technology – Personal information security specification national standard[39] explicitly refers, among others, to "*details of browsing behavior*" and "*information about personal devices*" as examples of personal information. Appendix B of the same national standard refers to "*webpages browsing details*" as being sensitive personal information.[40] The use of cookies[41] is therefore subject to the PIPL.

The consent of data subjects concerned must by way of general principle be secured prior to use of cookies unless the processing of the personal information at stake can rely on another lawful basis (Article 13 of the PIPL). According to Article 14 of the PIPL, consent must be fully informed and given in a voluntary and clear fashion. Specific consent shall be secured from data subjects if sensitive personal information is concerned.

For the purpose of obtaining a valid consent, Article 17 of the PIPL states that data subjects must be informed by the personal information processor[42] of the following elements, in a distinguishable form, in a clear and plain language and in a sincere, accurate and complete fashion:

(a) the identity and the contact details of the processor (save otherwise exempted by applicable law or regulation on the ground of confidentiality);
(b) the purpose, modality of processing, the categories of the personal information concerned and retention period for the personal information;
(c) the modalities and procedure whereby the data subject may exercise its rights under the PIPL;
(d) other information requested by law and regulation as may also be further specified by future legislation.

Where any of the above information is provided by the personal information processor through their established rules of processing of personal information (similar to the privacy notices provided for under the GDPR), these rules must be made available to the public, easy to access and store. On top of the information mentioned above, if sensitive personal information is involved, the processor must additionally inform data subjects of the necessity of processing their personal information and the potential impact of such processing.

Article 16 of the PIPL states that personal information processors cannot refuse to provide a product or service to individuals on the ground that they do not consent to the use of cookies (i.e. processing of their personal information) or they withdraw their consent, unless the use of these cookies is indispensable for providing the product or service.

Where the use of cookies is offered by an overseas personal information processor, the PIPL shall apply in the following circumstances:

(a) the processing (in an overseas jurisdiction) aims to supply products/provide services to individuals in China;
(b) behavioral analysis and assessment of individuals in China;
(c) other activities provided by Chinese law and regulation as may also be further specified by future legislation.

Where the use of cookie involves cross border transfer of personal information or the processing of sensitive personal information, the personal information processor must conduct a personal information protection impact assessment beforehand and keep a record of the processing.

D. United Kingdom

In May 2011, the UK became the first EU Member State to implement the amended Article 5(3) requiring notice and consent into national law, through amendments to Regulation 6 of the Privacy and Electronic Communications (EC Directive) Regulations 2003 (Regulation 6 or PECR). In implementing Article 5(3)'s consent requirements, the UK Government also imported additional clarification language from Recital 66 of the Citizens' Rights Directive. This acknowledged that individuals' consent to cookies can be expressed through appropriate browser or other application settings.

The key elements of this requirement are articulated in Regulation 6 as follows:

38. With the participation of Yiting Fei and Anling Zhang.
39. GB/T 35273-2020.
40. "Sensitive personal information" refers to personal information that, once leaked or illegally used, will easily lead to infringement of the human dignity or harm to the personal or property safety of a data subject.
41. Under the above quoted national standard there is no distinction between "session cookies" and "persistent cookies".
42. The term "personal information processor" used in the PIPL or "processor" in this document is the equivalent of "data controller" under the EU General Data Protection Regulation ("GDPR").

> *(1) (...) a person shall not store or gain access to information stored, in the terminal equipment of a subscriber or user unless the requirements of paragraph (2) are met.*
>
> *(2) The requirements are that the subscriber or user of that terminal equipment: (a) is provided with clear and comprehensive information about the purposes of the storage of, or access to, that information; and (b) has given his or her consent (...).*
>
> *(3A) For the purposes of paragraph (2), consent may be signified by a subscriber who amends or sets controls on the internet browser which the subscriber uses or by using another application or programme to signify consent.*

In addition and in line with the e-Privacy Directive, Regulation 6 of the PECR also introduces an exemption to the main rule that states:

> *(4) Paragraph (1) shall not apply to the technical storage of, or access to, information: (a) for the sole purpose of carrying out the transmission of a communication over an electronic communications network; or (b) where such storage or access is strictly necessary for the provision of an information society service requested by the subscriber or user.*

Despite the UK's departure from the European Union, at present the PECR requirements and exemptions remain unchanged. Therefore, the guidance provided by the Information Commissioner's Office (ICO) in this respect also remains unchanged. According to this guidance, in practice consent is not required in respect of the following:

- Cookies used to remember the goods a user wishes to buy when they add goods to their online basket or proceed to the checkout on an internet shopping website.
- Session cookies providing security that is essential to comply with data protection security requirements for an online service the user has requested (e.g. online banking services).
- Load-balancing cookies that ensure the content of your page loads quickly and effectively by distributing the workload across several computers.

However, the ICO states that it is still good practice to provide users with information about these cookies, even if consent is not needed. The ICO has not undertaken an aggressive enforcement stance on cookie consent compliance, but it has laid out clear expectations as to what amounts to compliance with these rules in the UK.

In this respect, the use of cookie walls as a blanket approach to restrict access to a service until users consent will not comply with the cookie consent requirements. The ICO views this approach as inappropriate if the use of a cookie wall is intended to require, or influence, users to agree to their personal data being used by a business or any third parties as a condition of accessing its service, as a user has no genuine choice but to accept cookies.

Implied consent is also no-go. Statements such as 'by continuing to use this website you are agreeing to cookies' should not be used as they do not meet the requirements for valid consent required by the UK GDPR. Pre-ticked boxes or any equivalents, such as sliders defaulted to 'on', cannot be used for non-essential cookies. Users must have control over any non-essential cookies and they must not be set on landing pages before consent is obtained.

The ICO also views consent mechanisms that emphasise that users should 'agree' or 'allow' cookies over 'reject' or 'block' as non-compliant. It calls this 'nudge behaviour' which influences users towards the 'accept' option. Consent mechanisms which incorporate consent controls in a 'more information' section rather than as part of the initial banner / pop out or other solution are also deemed non-compliant on the basis that they do not allow users to make a choice before non-essential cookies are set.

Looking forward, the UK Government has signalled a change to the rules applicable to cookies. Although the ongoing post-Brexit data protection reform is currently on hold, a number changes are expected to take place over the coming months. For example, there is likely to be an expanded range of exemptions to the consent requirement including:

(a) for the purpose of collecting statistical information about an information society service in order to improve that service;
(b) for enabling the way in which a website appears or functions in order to adapt to the preferences of the user;
(c) for the installation of necessary security updates to software on a device;
(d) to identify the geolocation of an individual in an emergency situation.

All of this seems to indicate that while at present the UK framework in this area is entirely aligned with the EU's, the cookie consent compliance requirements are likely to be softened and while they may not disappear altogether, harsh enforcement action by the ICO is also unlikely in this space.

PIN CODE
REVUE INTERNATIONALE DE LA PROPRIÉTÉ INTELLECTUELLE ET DU DROIT DU NUMÉRIQUE

#13 - JANVIER 2023

RPIN

Lorsqu'une décision jurisprudentielle est citée et que celle-ci est disponible dans notre base de données LexNow (www.lexnow.lu), vous retrouverez la Référence /ID en note de bas de page permettant un accès simplifié et direct au texte intégral sur LexNow.

Legitech Sàrl
10A, Z.A.I. Bourmicht
L-8070 Bertrange
T +352 26 31 64-1
www.legitech.lu

MADE IN LUXEMBOURG

LEGITECH *éditeur juridique*

PERIODIQUE

POST LUXEMBOURG

Envois non distribuables à retourner à: L-3290 BETTEMBOURG

PORT PAYÉ PS/765