An Coimisiún um Chosaint Sonraí
Data Protection Commission

Report by the Data Protection Commission on the use of cookies and other tracking technologies

Following a sweep conducted between August 2019 and December 2019

Report dated: 6 April 2020

Regulation 5 of the ePrivacy Regulations

Regulation 5 of the European Communities (Electronic Communications Networks and Services)(Privacy and Electronic Communications) Regulations 2011 (S.I. No. 336 of 2011) ('the ePrivacy Regulations') protects the confidentiality of electronic communications.

The ePrivacy Regulations in Ireland transpose the European ePrivacy Directive 2002/58/EC, as amended by 2009/136/EC, into Irish law. As this is an EU directive, each Member State has its own legislation transposing it into its national laws.[i]

Regulation 5(3): A person shall not use an electronic communications network to store information, or to gain access to information already stored in the terminal equipment of a subscriber or user, unless

(a) the subscriber or user has given his or her consent to that use, and

(b) the subscriber or user has been provided with clear and comprehensive

information in accordance with the Data Protection Acts which—

(i) is both prominently displayed and easily accessible, and

(ii) includes, without limitation, the purposes of the processing of the information.

Regulation 5(4): For the purpose of paragraph (3), the methods of providing information and giving consent should be as user-friendly as possible. Where it is technically possible and effective, having regard to the relevant provisions of the Data Protection Acts, the user's consent to the storing of information or to gaining access to information already stored may be given by the use of appropriate browser settings or other technological application by means of which the user can be considered to have given his or her consent.

Regulation 5(5): Paragraph (3) does not prevent any technical storage of, or access to, information for the sole purpose of carrying out the transmission of a communication over an electronic communications network or which is strictly necessary in order to provide an information society service explicitly requested by the subscriber or user.

Background

In August 2019, the Data Protection Commission (DPC) commenced an examination of the use of cookies and similar technologies on a selection of websites across a range of sectors, including media and publishing, the retail sector, restaurants and food ordering services, insurance, sport and leisure and the public sector.

We chose popular websites operated by some of the most well-known organisations across these sectors. We also included controllers whose use of cookies had come to the attention of the DPC through complaints from members of the public, or through our own observations of how information about cookies and tracking technologies was presented, or appeared to be lacking, on those sites.

The purpose of the sweep survey was to request information to allow us to examine the deployment of such technologies and to establish how, and whether, organisations are complying with the law. In particular, we wanted to examine how controllers obtain the consent of users for the use of cookies and other tracking technologies.

We did not undertake a broader examination of the adtech industry or the real-time bidding advertising framework as part of this sweep as these issues are the subject of separate inquiries by the DPC. Nevertheless, it was evident from the examination of the types of tracking technologies and cookies in use that advertising technology and tracking are core to the business models of many of the websites examined.

Commentary

Of the 40 controllers asked to participate, one was subsequently given a deferral on the basis that it was about to roll out an entirely new website. One controller did not respond to any of the DPC's correspondence or reminders and the DPC may consider further action in that regard.

The standard of consent that controllers must obtain from users or subscribers for the use of cookies must now be read in light of the GDPR standard of consent, i.e. it must be obtained by means of a clear, affirmative act and be freely given, specific, informed and unambiguous.

There was a good level of cooperation with the sweep and most controllers were keen to demonstrate compliance. Just under a third of the controllers signalled that they had either identified possible improvements to their practices or that they were endeavouring to comply with the regulations and were keen to have updated guidance from the DPC. Two controllers specifically stated that they were aware that they might not currently be compliant.

The quality of information provided to users in relation to cookies varied widely. Some controllers' websites provided detailed and layered information about the technologies in use, and others provided little detail about the use of cookies, or about how to reject them.

We also established that many controllers are setting a wide range of cookies as soon as a user lands on their website, without any engagement by the user with a consent management platform or cookie banner. These included third-party cookies from social media companies, payment providers and advertisers, which enable the browsing habits and online (and potentially offline) behaviour of individuals to be extensively tracked and monitored, even across multiple devices and sessions.

Many controllers categorised the cookies deployed on their websites as having a 'necessary' or 'strictly necessary' function, where the stated function of the cookie appeared to meet neither of the two consent exemption criteria set down in the ePrivacy Regulations/ePrivacy Directive. These included cookies used to establish chatbot sessions that were set prior to any request by the user to initiate a chatbot function. In some cases, it was noted that the chatbot function on the websites concerned did not work at all.

It was clear that some controllers may either misunderstand the 'strictly necessary' criteria, or that their definitions of what is strictly necessary are rather more expansive than the definitions provided in Regulation 5(5).

The regulation provides that the requirement to obtain consent to store information, or to gain access to information already stored in the terminal equipment of a subscriber or a user "*does not prevent any technical storage of, or access to, information for the sole purpose of carrying out the transmission of a communication over an electronic communications network or which is strictly necessary in order to provide an information society service explicitly requested by the subscriber or user*".

In some cases, controllers also had tracking technologies such as Facebook pixels embedded in their websites, but they did not list these in their responses to the sweep and limited their list of cookies to http browser cookies only. It was not clear, therefore, whether some controllers were aware of some of the tracking elements deployed on their websites – this was particularly the case where small controllers had outsourced their website management and development to a third-party.

There was some level of awareness, particularly among larger controllers, of recent or then-pending rulings by the Court of Justice of the European Union (CJEU) in the ePrivacy area, which may impact on their practices. Some indicated they were reassessing issues of joint controllership that may arise in respect of the use of third-party plugins and social 'like' buttons in light of the *Fashion ID* judgment of 29 July 2019.

This included, in some cases, reassessing their contractual relationships with third parties.

In October, shortly after we commenced the sweep, another significant judgment from the CJEU in the *Planet49* case clarified that consent for the placement of cookies is not valid if it is obtained by way of pre-checked boxes which users must deselect to refuse their consent.

Ten (26%) of the controllers who responded were found to have pre-checked boxes to signal consent to cookies, including to marketing, advertising and analytics cookies. These controllers will need to act expeditiously to amend their interfaces, which it is clear do not comply with EU law. Some further engagement with these controllers will be required in order to draw these issues to their attention.

Many controllers relied on implied consent to set cookies, or they directed users to the browser settings to control cookies. It appears from the responses, and from the information provided in relation to cookies on most of the sites, that controllers read Regulation 5(4) to mean that a user's consent may be inferred from their browser settings. The Article 29 Working Party, however, has clarified that this provision in the ePrivacy Directive (as transposed in Regulation 5(4)) is not an exception to Article 5(3), but "rather a reminder that, in this technological environment, consent can be given in different ways – where technically possible, effective and in accordance with the other relevant requirements for valid consent. In this context, a relevant question is to determine the conditions under which the browser settings will meet the requirements of Directive 95/46/EC [and now the GDPR] and thus constitute a valid consent…" The opinion goes on to say that the Article 29 Working Party considers that this will happen "*in very limited circumstances*".[ii]

There were also examples of pre-checked boxes which opted users in to analytics and marketing cookies by default, but with the controller failing to honour any choice expressed by the user if they unchecked the boxes. In one particular case, the controller had implemented a Cookiebot consent management tool which had pre-checked boxes for 'preference', 'statistics' and 'marketing' cookies. The user unchecked all these boxes and proceeded to browse the site, which resulted in a number of performance and marketing-related (audience segmentation) cookies being set without any consent. There was also a payment-related third-party cookie with a 10-year lifespan set without any consent and without the user having added any items to the shopping basket.

A lack of clarity on how users could reject or later withdraw their consent to cookies was also a feature on many sites.

We also noted user interfaces where a cookie banner was displayed offering no choice other than 'accept' without any link to additional information about cookies, and with

the cookies policy or privacy policy in the page footer obscured by the banner. These practices are not only poor from a user interface perspective—they actively obstruct users from obtaining the information they require in order for their consent to be considered freely given and unambiguous.

About 15 of the 38 controllers who responded signalled either that they were aware they may not be compliant with the existing regulations, or that they had identified improvements that they could make to their websites in order to demonstrate compliance. A number of them have taken steps to amend their practices on foot of this sweep, including the removal of unnecessary or unsecure cookies they identified in the course of the exercise.

However, it is our view that almost all of the sites continue to have compliance issues, ranging from minor to serious.

Methodology

The investigation team carried out a desktop examination of each controller's response to the sweep, assessing the information provided and analysing its compliance with the current S.I. 336/2011 ('the ePrivacy Regulations') and to establish whether consent for non-exempt cookies or tracking technologies was being obtained in line with GDPR requirements (i.e. freely given, specific, informed and unambiguous).

Each website was also examined individually in a clean (i.e. with cookies cleared) browser to ascertain in so far as was possible whether the controller's description of its cookie activities and its compliance matched the actual activity and the information presented to users in the interface.

For the purposes of this phase of the sweep, the investigation team therefore was relying on the observable activity in browsers, assessment of the language and user interfaces (UX) deployed by the controllers, analysis of the existing legal framework, and the controllers' self-asserted compliance with the legislation.

The investigation team classified each controller using a simple RED, AMBER, GREEN coding system.

> GREEN indicated a very good response, substantially compliant, any concerns straightforward and easily remedied.
>
> AMBER signalled a good response and approach to compliance, but at least one serious concern.
>
> RED classification was a poor or incomplete response or questions not understood, with several serious concerns.

Assessing compliance/non-compliance by the 38 respondents

Twenty of the controllers examined were given an AMBER grading. Three were given a borderline AMBER to RED grade.

Twelve controllers were given a RED grading, based not only on the very poor quality of their responses but also on bad practices with cookie banners, the setting of multiple cookies without consent, badly designed cookies policies or privacy policies, and a lack of clarity about whether they understood the purposes of the ePrivacy legislation.

Just two controllers were given a GREEN rating, with one a borderline GREEN to AMBER.

The majority of the 38 controllers examined were found to have potential compliance issues, particularly in relation to reliance on implied consent for setting non-exempt cookies, the setting of cookies on landing without any engagement by the user with consent banners or other tools, lack of choice for users to reject all cookies, bundling of consent for all purposes and the possible misclassification of cookies as 'necessary' or strictly necessary when they may not avail of one of the two exemptions provided in the ePrivacy Regulations.

Implied consent

About two thirds of the controllers were specifically relying on a model of "implied consent" to set cookies, based on the wording of their cookie banners (e.g. "by continuing to browse this site you consent to the use of cookies") Some appeared to be drawing on older, but no longer extant, guidance published by the DPC that indicated consent could be obtained "by implication", where such informational notices were put in place. (Current guidance on the DPC's website does not make any reference to implied consent, but it also focuses more on user controls for cookies rather than on controller obligations.)

These controllers relying on implied consent used various forms of words in their cookie banners and notices to the effect that by continuing to browse the site, a user will be deemed to have consented to the use of cookies.

DPAs in France, Germany and the UK consider that such activity does not amount to consent and that for consent to be valid, it must be freely given, specific, informed and unambiguous. Recent guidance published by the Spanish DPA, however, indicates that users may give their consent to cookies by means of "a clear affirmative action" such as scrolling a website or clicking a link. The DPC does not consider that continuing to scroll a site (at which point a cookie banner with which the user has not engaged may disappear), or that clicking any links or elements on a web page or app interface, may

constitute freely given, specific, informed and unambiguous consent to the setting of cookies.

Non-necessary cookies set on landing

In the case of almost all the websites apart from one, cookies were set immediately on landing. This included in many cases cookies that do not benefit from one of the available consent exemptions in the regulations.

Most websites with cookie banners had an interface that favoured an 'accept' option, without an option to 'reject' cookies. Even where they did have an option to learn more about cookies, in many cases this did not include a layered option to accept or reject cookies by function. A so-called 'nudging' approach to the web design is therefore common, with users effectively forced into accepting all cookies.

Tools

A lack of tools for users to vary or withdraw their consent choices was a factor on most of the reviewed sites, despite the deployment of third-party vendors' consent management platforms by some controllers. OneTrust and Cookiebot were the two most common CMPs in use.

Most controllers appeared to be deploying a specific consent cookie to record that a user has consented to cookies. These consent cookies mostly had lifespans of about a year.

The use of persistent cookies to record a user's consent state and their cookie preferences is potentially confusing for data subjects where there are no visible tools on the website to facilitate them to later withdraw or vary their consent. A persistent consent cookie may be stored in a manner where it is not immediately clear to the user or subscriber that they may have visited the site before and that a consent preference has already been recorded for them. The Article 29 Working Party has noted the practical problems related to obtaining consent, particularly if consent is necessary every time a cookie is read for the purposes of delivering targeted advertising. [iii]

However, WP29 also recommends limiting the scope of the consent to a period of time, for example one year. It was not always evident on the 38 websites, particularly where the controller deployed an "implied" consent model, that the consent state had been recorded by means of a cookie on a previous visit. This made it all the more difficult for a user, even with some knowledge of how to adjust the browser settings or of how to remove cookies, to vary their consent or to reject cookies on a second or subsequent visit. One obvious design solution to allow users vary their cookie consent would appear to be a cookie button (or a 'radio button') which reveals sliders or on/off options.

Banners and interfaces

Badly designed—or potentially even deliberately deceptive—cookie banners and consent-management tools were also a feature on some sites.

Two controllers were using the Quantcast consent management platform.

Examining how this Quantcast CMP was deployed by controllers solely within the scope of this cookies sweep, the interface as implemented was confusing and potentially deceptive. In the case of one website, a feature purporting to link to the consent management interface, as outlined in the controller's responses to the sweep, did not work.

In the case of one of the controllers using Quantcast, the sliders purporting to give the user control over the cookies they accept or reject are set to red by default. Changing them to the opposite position highlights them in green. However, the settings are not labelled as either ON or OFF. Logic and normal design convention would suggest the red setting to be the OFF position. However, the slider interface is presented beneath two black buttons at the top of the screen, one reading **REJECT ALL** and the other **ACCEPT ALL**. Clicking on the REJECT ALL button has no effect. In order to proceed to the site, the user must click either **ACCEPT ALL**, or **SAVE & EXIT**. It is not at all clear whether clicking **ACCEPT ALL** overrides the slider settings.

Accessibility

Not all users will experience a website or app in the same way and some interfaces with coloured buttons and sliders may be confusing for those who have colour blindness, for example.

It is estimated that red-green colour blindness affects up to 8% of males and between 0.5% and 1% of females. Some of the websites we examined had implemented sliders with red and green colour schemes, but which were not marked clearly to denote the ON and the OFF positions.

This means that an interface with binary RED/GREEN choices may prove difficult for some people to navigate as they may find it hard to distinguish between the colours.

Recommendation: Controllers must give consideration to accessibility issues when designing their browser and mobile user interfaces.

As best practice, sliders or check boxes should be clearly marked as ON or OFF, even if they also have a binary colour choice, in order that the user is not forced to guess at their functionality.

Controllers' assessment of their compliance

About 15 of the 38 controllers who responded signalled either that they were aware they may not be compliant with the existing ePrivacy regulations, or that they had identified improvements that they could make to their websites in order to demonstrate compliance. It was clear from some responses that even the changes proposed by controllers may not serve to bring them into full compliance, particularly as regards the use of implied consent, the inadequacy of the information provided to data subjects about the types of cookies and tracking technologies in use, and the lack of a clear means of rejecting non-necessary cookies or of varying consent at a later point.

A flavour of the responses

- One controller stated it believed it was compliant, but it confused the ePrivacy Regulations (S.I. No. 336/2011) with the proposal for a new EU ePrivacy Regulation, which has yet to be agreed and finalised. Indeed, a number of controllers made reference to the proposal for a new ePrivacy Regulation in their responses and how they wished to "future proof" their compliance. However, this essentially appears to involve the controllers anticipating the introduction of features or interfaces that may not be compliant with the current legislation.
- One controller believed the deployment of the Cookiebot CMP rendered its website compliant with the regulations. The use of a third-party tool to manage cookie consents does not in itself guarantee the controller is compliant. As with privacy policies and cookie policies, such tools cannot work on a one-size-fits-all basis: they must be tailored specifically to the needs of each controller and they **must** do what they purport to do. The buttons and sliders must function as presented and any consent preferences recorded must be accurately recorded and respected.
- A large retailer accepted that it was not compliant with the current legislation but stated that it was planning to implement a new CMP by Q1 of 2020.
- In the case of another large controller in the retail sector, it did not appear to be fully aware of the functions of some of the third-party cookies set on its site, noting in one case that the cookie was "most likely used for demographic profiling and targeting for advertising". Where controllers are utilising such technologies on their own websites, the responsibility lies with them to be aware of their purpose and functionality.
- A controller in the banking sector confirmed that it may combine information entered by users for the purposes of making calculations on lending products or for other reasons with targeting cookies for advertising purposes.
- A different controller in the banking industry indicated it was aware that reliance on implied consent for the setting of cookies may not be compliant.

- A controller in the restaurant sector stated that it believed consent was not required for setting cookies, despite the fact that the legislation and its purposes were set out in the letter sent to all controllers on 15 August 2019. This controller and a number of others in the restaurant sector (all of which utilise the same underlying ordering platform), failed to adequately answer the DPC's questions about their use of cookies and other trackers.
- A number of controllers in the sport sector showed a good approach to compliance. On foot of the sweep, one controller identified a number of actions, including that it would delete any unnecessary or unused cookies placed on user devices. It said many of these were unsecure cookies and that they would cease to be placed in Q1 2020 once its online shop moved to a new platform managed by an independent data controller. It also implemented a consent management tool.
- Controllers in the media and publishing sectors, the banking and finance sectors and the health insurance sector had a significant number of third-party trackers, including advertising trackers which track users across the internet. One controller had approximately 150 third-party advertising trackers as well as dozens of third-party analytics cookies set without consent.
- Not all controllers appear to have provided information about tracking in JavaScript, so the extent of this type of tracking cannot be clearly assessed in this exercise. One controller indicated it uses the Facebook SDK (software development kit) to allow it to add social plugins, a Facebook login and other Facebook features. Other controllers may also be using Facebook SDK.
- One media company also noted it used a third-party GPS tracking cookie to register a unique ID on a mobile device to enable tracking based on GPS location. Any cookies or tracking technologies that involve the processing of data on the precise location of a user or a device require consent.

Trackers on health-related sites

- Third-party tracking on a number of health-related websites is a particular cause for concern, especially in the case of controllers who may have already built explicit profiles of known users/customers (such as in a health insurance context). For example, health insurance websites were found to be using advertising and targeting cookies, including cookies set by the Google-owned DoubleClick.
- One controller in this sector described a third-party advertising cookie as follows: *"This DoubleClick cookie is generally set through the site by advertising partners, and used by them to build a profile of the website visitor's interests and show relevant ads on other sites. This cookie works by uniquely identifying your browser and device."*

- Another health-related controller uses targeting cookies, with Quantserve cookies used to send users "relevant ads" when they visit other sites subsequently. The website also uses Hotjar, which analyses where users click and scroll on the website. The controller uses targeting cookies to track sales when users click on ads delivered to them on other websites.
- One public body uses so-called floodlight tags (DoubleClick and Facebook pixels) "to support advertising performance tracking". It provides choices by means of two sliders (set to red) to accept "cookies that measure website use" and "cookies that help with health campaigns". Users are informed that these cookies are used to tell the controller if the user has seen its ads on social media, such as Facebook or Twitter. There was insufficient granularity in the explanations of the purposes of these cookies and also in the controls for accepting or rejecting them. It was not clear which types of cookies were being set and which of them may not have met the criteria for exemption from consent in Regulation 5(5).
- Such lack of clarity about its use of cookies is concerning from a public sector organisation providing health-related information. While such an appeal to the altruism of users of a health website to give consent for cookies that "help with health campaigns" is not necessarily prohibited, the nature of these cookies, their exact purposes and the third parties with whom information will be shared based on the user's consent must be outlined prior to setting the cookies. Where such cookies may involve the processing of special category data based on inferences drawn from a person's browsing patterns on a website, their previous use of the site, or linked data from other sources, this consent must be **explicit.**
- The same organisation was also found to be setting cookies it classified as strictly necessary with a lifespan of "forever". The Article 29 Working Party has recommended that cookies that are exempt from consent "*should have a lifespan that is in direct relation to the purpose it is used for, and must be set to expire once it is not needed, taking into account the reasonable expectations of the average user or subscriber*".[iv]
- We are concerned that is possible that special category data, such as details of illnesses or conditions a user may search for on such sites, is being shared with parties such as Google and Facebook through the use of either explicit profiles of logged-in customers, or through predictive profiles based on unique identifiers. In these cases, the controller may potentially be processing special category data and sharing it with third-parties, including advertisers, without a lawful basis.

Pre-checked boxes

Ten of the 38 controllers were using pre-checked boxes or sliders on their websites. In the case of most of the controllers, consent was also 'bundled' – in other words, it was not possible for users to control consent to the different purposes for which cookies

were being used. This is not permitted, as has been clarified in the *Planet49* judgment. Consent does not need to be given for each cookie, but rather for each purpose. Where a cookie has more than one purpose requiring consent, it must be obtained for all of those purposes separately.

In the case of at least one website it was observed that unchecking the 'preferences', 'statistics' and 'marketing' checkboxes on the homepage CMP (Cookiebot) had no function and the cookies were set anyway once the user began browsing the site.

Planet49 judgment: On 1 October 2019, the Grand Chamber of the Court of Justice of the European Union delivered its judgment in the *Planet49* GmbH case.

This judgment clarified that consent is not validly constituted if, in the form of cookies, the storage of information or access to information already stored in a website user's terminal equipment is permitted by way of a pre-checked checkbox which the user must deselect to refuse his or her consent.

The ruling also clarified that the requirements for consent are not to be interpreted differently according to whether the information stored or access on the user's device is personal data.

Controllers who had deployed consent-management tools or cookie banners and notices with pre-checked boxes or sliders set by default to on, should now be required to address this matter without delay.

The judgment also makes clear that the indication of the data subject's wishes must, inter alia, be 'specific' in the sense that it must relate "specifically to the processing of the data in question and cannot be inferred from an indication of the data subject's wishes for other purposes". This means that the so-called 'bundling' of consent for all purposes for which cookies or other tracking technologies are used, is not permitted.

Controllers should also take careful note of the fact that whether or not the cookies deployed are viewed as "containing" or constituting personal data in themselves, consent is required prior to setting them unless they benefit from one of the two consent exemptions provided for in the ePrivacy Regulations at Regulation 5(5).

Nevertheless, they should also be aware that the further processing of information obtained through cookies and other tracking technologies, including unique identifiers and device information, may constitute personal information and that its processing is subject to the GDPR.

Analytics

Analytics cookies are used to measure how users use a website, for example how long they spend on each page, how they navigate a website and what content they engage with and for how long. They are also used to distinguish between users and to measure return visits to a website. So-called 'first party' analytics are used only by the website controller, or a processor acting on its behalf, to measure this engagement. Third-party analytics cookies are used by parties other than the controller.

All the sites examined deploy analytics cookies, with most using first and third-party analytics. Google Analytics cookies were the most commonly used.

By far the most extensive third-party tracking was noted on the websites of the main media publishers, with most of them embedding audio and video content as well as social media trackers for adtech purposes.

Pixels and other trackers

Pixels, also known as web beacons or pixel tags are often embedded in websites or in emails in order to monitor or track a user's actions. These are often in the form of a single, clear pixel in the website code and they are invisible to the eye. They can be used, for example, to tell when a user opens an email or clicks on content within an email and controllers may use them to measure user engagement with their content and to help them deliver personalised content.

If a user of a social network such as Facebook is logged into their account when they visit a site with a Facebook pixel, Facebook can connect their browsing behaviour on that site to personal data it processes on that user. The website controller can, in turn, use this information on an aggregated basis to place ads on Facebook based on its own users' interests or inferred interests.

Although all controllers were asked to list all cookies deployed on their websites, including all third-party assets and plugins, only a small number confirmed that they used pixels on their websites and instead listed http cookies only.

As these tracking devices could not generally be observed in the course of a desk-based study, the investigators cannot be certain how many of the sites may contain pixel tags or other trackers which cannot be cleared in the normal way along with ordinary http (browser) cookies. However, Facebook provides its own plugin for the Chrome browser to assist developers in troubleshooting their implementation of the pixel on websites. Using this tool, (Facebook Pixel Helper) it was possible to observe that a Facebook pixel was in operation on several of the sites examined.

Social buttons and third-party plugins

Tools known as plug-ins store and access cookies in the user's terminal equipment to allow, for example, social networking sites to identify their members when they interact with the website or share its content. However, once the cookies associated with these plug-ins are 'dropped' on the computer or device when a user visits a website, they can track users and also non-users of these social networking sites across their online browsing habits.

Such plug-ins are typically recognisable as 'like' buttons, follow buttons, or other social media sharing tools visible as a branded icon on the web page – the Facebook 'like' button probably being the most recognisable of these.

Thirty-four of the 38 controllers examined deployed third-party plugins on their websites. The main ones in use were Facebook, Twitter, Instagram and LinkedIn, with a small number also using a TripAdvisor widget linking to their TripAdvisor reviews. Two controllers had social buttons for Google +.

Google + was deprecated in April 2019 and that, as such, these tools were obsolete. (The controllers appear to have removed these G+ buttons since they responded to the DPC sweep.)

Main concerns

The issues that stand out most starkly in the analysis of the responses, and our desktop examination of the websites in question, are the following:

- Ten (26%) of the controllers who responded were found to have pre-checked boxes to signal consent to cookies, including to marketing, advertising and analytics cookies.
- The use of implied consent to set cookies, including in some cases extensive tracking, marketing and analytics cookies.
- Two thirds of the controllers examined specifically stated their reliance on implied consent and/or the user controlling cookies via their browser settings. Cookie banners that state the controller will assume the user, by continuing to use the site, is happy with the use of cookies, are widespread.
- Inability to vary or withdraw consent was also common. Where a cookie banner has been presented and the settings are chosen, or cookies are accepted, the sites' user interface often has no visible functionality to vary consent settings at a later stage. It appears that some controllers are using persistent cookies to read the consent state for a set period of time and that these are impossible to clear through the commonly understood methods within the browser settings.

- Identifying cookies as 'necessary' or 'strictly necessary' where they clearly do not benefit from either of the two very narrow consent exemptions provided in Regulation 5(5) was also extremely common.
- Poorly designed cookie banners and poor information in relation to cookies and their purposes, bundling of consent for all purposes, a lack of clarity on how a user may withdraw or vary their consent at a later stage.
- A lack of understanding of the purposes of the cookies legislation, which is to protect the private sphere of users in their communications.
- Confusion between the ePrivacy Regulations 2011 and the proposed new ePrivacy Regulation, which has not been agreed and which appears highly unlikely to be agreed in the short term.
- A number of controllers referred to the use of cookies and their partnerships with third parties as being fundamental to their ability to continue to provide their services free of charge to users. While this may be the case, where such partnerships involve cookies and/or the processing of personal data, the processing is subject to the ePrivacy regime and/or the GDPR, as appropriate and controllers are expected to comply will all applicable rules and legislation. There are differing views among other DPAs about whether blocking a user's access to a website on the basis that a user has not consented to cookies is compliant. We are of the view that users should not suffer any detriment where they reject cookies or other tracking technologies, other than to the degree that certain functionality on the websites concerned may be impacted by that rejection.
- Some controllers indicated they were studying the implications of the July 2019 Fashion ID judgment of the Court of Justice of the European Union as it pertained to possible joint controllership issues. A number of controllers, however, had not taken this judgment into account in their responses or practices and some appeared to be of the belief that they had no responsibility for any third-party cookies or tracking on their websites.
  (The judgment makes clear that the operator of a website that embeds a social plugin (such as a 'like' button or a social sharing tool) that causes the user's browser to request content from the plugin provider, and to that end, to transmit to that provider the personal data of the visitor to the provider of the plugin, can be considered to be a controller.)
- One controller listed the purpose of one Google Analytics cookie as being "used to determine a user's inclusion in an experiment and the expiry of experiments a user has been included in". This cookie is set before a user gives consent.
- One travel website deployed a cookie with a two-year life span used to uniquely ID a user's browser and device for the purposes of displaying a journey planner. This cookie was set without consent on landing. While such functionality may be

helpful to some users, or indeed desired by some users, these cookies are not strictly necessary and they require consent. The duration of the operation of that consent to remember the user for the purposes of their journey planning should also be clear to the user when they give it.

- A controller in the publishing sector was setting analytics cookies when a user merely scrolled down the landing page. It also placed a unique user ID cookie with a lifespan of 10 years. It is not reasonable to consider that a user has given consent to this merely by moving a mouse over a screen. This controller also has a consent management tool that appears not to work and which has pre-checked boxes for advertising cookies.
- Another publisher confirmed that it combines a person's registration details with analytics cookies to identify which pages they have read on the site. This involves the processing of personal data in a manner which allows the profiling of individuals. Any cookies used to facilitate such profiling, or data derived from cookies which facilitates such profiling, require consent. In addition, such processing where the linking of different datasets significantly contributes to, or is used for profiling or behavioural analysis of individuals, requires a data protection impact assessment. The circumstances in which a DPIA is mandatory have been published by the DPC on its website.
- A public authority was setting cookies without consent and had implemented pre-checked boxes on its website. The cookies deployed included a YouTube cookie that placed a unique ID on a mobile device to track the GPS location.
- One health insurer deployed a third-party Google Analytics cookie used by Google Analytics to determine if the visitor is "involved in their marketing experiments". A Google pixel tracker also "tracks the visitor across devices and marketing channels".

  Given that a Facebook cookie to deliver real-time bidding for ads from third party advertisers was also set on this website, it appears likely users are being targeted based on what they search for, including health information. The likelihood that the websites and third parties are processing special category data on foot of a user's searches or other interactions with health websites on which trackers are embedded is high. Where controllers are processing personal information in cookies, or derived from cookies, including where the data is combined with explicit profiles or logins, the processing of special category data may only take place with the **explicit** consent of the user.
- One large retailer stated that it may combine data collected through cookies in the browser or other devices with other data it has collected, such as in-store purchases and registered loyalty card data.

Best and worst examples

On the basis of our findings in this sweep, the worst sector in terms of poor practices and, in particular, poor understanding of the ePrivacy Regulations and their purpose, appeared to be the restaurants and food-ordering sector.

It may not be coincidental that a number of these controllers were using the same underlying ordering platform and app. This was not known to the investigation team at the outset of the sweep.

Our assessment suggests this third party to be a data controller in its own right and a joint controller with the restaurant websites in relation to the personal data processed through its ordering systems. However, the website owners (some of them relatively small businesses) were of the understanding that the third-party ordering website was the sole controller in relation to their websites because they had signed over the management of their websites to that company.

This company is described as a data processor in a number of privacy policies examined in the course of this sweep.

The organisation claims several hundred customers in the restaurant sector in Ireland alone, and hundreds more across about a dozen countries. The DPC has received several complaints about the controller's practices with regard to the setting of cookies and the retention of personal data submitted when people use the platform to order food. We intend to have further engagement with this controller.

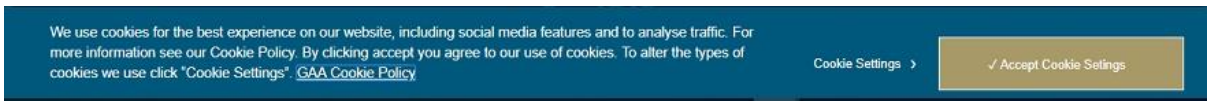
Good practices, bad practices

This is an example of a bad cookie banner:

"This website uses cookies to ensure you get the best experience on our website. (Learn more)...Got it!"

This is an example of a better cookie banner. However, it still emphasises the 'accept cookie settings' button over the function that brings the user to more layered information about the use of cookies. In general, layered information allowing users to consent to cookies or to reject them is good practice but the 'accept' option should not be emphasised over the option to change cookie settings or to reject them. The options should have equal prominence.

"We use cookies for the best experience on our website, including social media features and to analyse traffic. By clicking accept you agree to our use of cookies. To alter the types of cookies we use click 'Cookie Settings'."



Conclusions and recommendations

While only a small number of controllers were targeted to participate in this sweep, the examination of the 38 websites suggests that users of Irish websites are being tracked by third parties to a significant degree across their browsing habits and daily online activities.

Lacking even basic information or the ability to give unambiguous consent for the placement of tracking technologies or cookies on their devices, most ordinary users will not be aware of the extent to which they may be tracked across their devices at home and at work, and across their browsing, reading and social habits.

While they may not be tracked by name, the ability to track them by means of unique identifiers set through cookies or other technologies means they are being targeted as individuals and such targeting and/or profiling (after the point where cookies have been set) is subject to the GDPR where it may concern personal data.

Furthermore, it is apparent that websites providing health insurance and other health-related information may – inadvertently or otherwise – be sharing special category data with third parties in the adtech industry.

An investigation by the *Financial Times* in the UK in November 2019 found that some of the UK's most popular websites were sharing special category data, including medical symptoms, diagnoses, drug names and menstrual and fertility information with dozens of companies, including Google, Amazon, Facebook and Oracle, as well as with lesser-known data brokers and adtech companies. [v]

The ICO confirmed to the *Financial Times* its concerns about the processing of special category data in online advertising, as well as "the role that site owners and publishers play in this ecosystem".

It is notable that at least one of the health insurance websites examined in this sweep uses third party cookies from Hotjar to track user behaviour on the site. Ostensibly, this is to provide it with information on how people navigate the site and the menus. However, Hotjar may also capture video footage of precisely how a user navigates the site, including details of the text entered into boxes and search fields.

The investigation team surmises based on the information provided by these controllers, and based on examination of their sites and the cookies being set, that similar levels of sharing of personal data may be taking place via Irish websites.

Those controllers using pre-checked boxes will need to act expeditiously to amend their interfaces, which it is clear do not comply with EU law. Some further engagement with these controllers will be required in order to draw these issues to their attention. Ongoing and ad hoc engagement with other controllers where ePrivacy/cookies compliance issues are apparent will also be considered by the DPC.

The fact that bad practices were widespread even among companies and controllers that are household names suggests a more systemic issue that must be tackled firstly with the publication of new guidance, followed by possible enforcement action where controllers fail to voluntarily bring themselves into compliance.

A number of larger controllers referred in their responses to the ongoing negotiations at EU level on a proposal for a new ePrivacy Regulation to replace Directive 2002/58/EC. There were some references to controllers wishing to "future-proof" their websites by adopting some of the possible new requirements that might feature in any such legislation.

It must be clear to controllers that they are expected to comply with the current regime, pending any agreement at EU level on a proposal for a new regulation.

All positive steps towards compliance with the ePrivacy Regulations will ultimately benefit all data subjects using these websites and apps. However, the underlying processing of data enabled by cookies and other tracking technologies can only be addressed as part of a much wider examination of the entire adtech industry and ecosystem.

The DPC has today published new guidance for controllers and will allow a six-month time period for compliance, after which action up to and including enforcement action will be considered.

New DPC guidance and follow-up correspondence with the controllers who took part in the sweep will emphasise the following issues:

- Controller must remove any pre-checked boxes related to the setting of cookies.
- Ensure that their cookie banners are designed in such a way that they do not 'nudge' users into accepting cookies. An option to reject must have equal prominence in any banner or user interface.
- Ensure that no non-necessary cookies/non-exempt cookies are set on the landing page.

- Examine all cookies they have categorised as 'necessary' or 'strictly necessary' to determine whether they actually meet the strict conditions for either of the two exemptions set out in Regulation 5(5).
- The Article 29 Working Party opinion 4/2012 on the cookie consent exemption is still valid and should be studied by controllers. In particular, controllers should note the A29 opinion that the risk to data protection comes from the purpose(s) of processing rather than the information contained within the cookie.
- Controllers must ensure that consent is obtained for each purpose for which cookies are set. This does not mean that consent needs to be obtained individually for each cookie, but merely for the purpose for which it is being used.

  Consent may not be bundled, i.e. an "all or nothing" approach to accepting or rejecting cookies. Users must be able to reject non-necessary cookies and they must be able to vary their consent easily at any time via the website.
- Analytics cookies, targeting cookies and marketing cookies require consent. However, first-party analytics cookies are considered potentially low risk and it is therefore unlikely that they would be a priority for any formal action by the DPC.
- If a cookie is 'strictly necessary', its lifespan should be proportionate. Article 29 Working Party 04/2012 on the Cookie Consent Exemption 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 once it is not needed, taking into account the reasonable expectations of the average reader or subscriber. "This suggests that cookies that match the [consent exemption criteria] will likely be cookies that are set to expire when the browser session ends or even earlier.
- Privacy and cookie policies must always be visible and available to the user without them having to consent to cookies or dismiss a cookie banner. Non-necessary cookies should not be set prior to the user clicking on the cookie information and, where a link to a cookie policy is presented in a pop-up or cookie banner, the banner must not obscure the text of that policy.
- Users must always be able to withdraw consent or change permissions for cookies or other tracking devices. It should be as easy to withdraw consent as to give it.
- Privacy and cookie policies should be accurate and kept up to date. Using a template service to generate a privacy policy or cookie policy is a futile and cosmetic exercise. Similarly, controllers who have multiple websites must ensure that each of them has their own privacy policy which reflects the underlying reality of the processing.

- Controllers must examine the possible joint controller issues arising from the use of third-party assets and plugins. Where necessary, they must put in place controller-processor contracts, which must reflect the actual facts of the processing.
- Controllers must be aware that consent is required for non-necessary cookies whether or not personal information is processed. PII is not a concept recognised in EU law.
- The user interface needs to build in a clear option for users to change their cookie settings at any time, including where websites are using persistent cookies to store the user's "consent state" over a period of time. This could be accomplished, for example, by means of a settings tool or so-called radio button.
- The DPC recommends that users examine the checkboxes and sliders they use to allow a user signal consent. It should be very clear which setting is ON or OFF and how to ACCEPT and REJECT cookies. A user interface with sliders set to green or red, or other colours, may not provide sufficient clarity and it may result in accessibility issues for users with certain vision impairments.
- It is possible that some controllers are using device fingerprinting technologies which were not possible to observe in the course of this exercise. To the extent that any controller uses such technologies, they should be aware that Article 5(3) of the ePrivacy Directive (and by extension Regulation 5(3) of the ePrivacy Regulations 2011) is applicable. Opinion 9/2014 of the Article 29 Data Protection Working Party on the application of Directive 2002/58/EC to device fingerprinting should be studied in that regard.
- Controllers should be aware that the use of a consent management platform will not in itself ensure compliance with the legislation. They must ensure when deploying such tools that they do, in fact, work in the manner intended and that the tools and buttons on the user interface do what they purport to do. If a user checks or unchecks preferences, these preferences must be respected and recorded, as appropriate.
- Controllers must be aware that the processing of data which occurs subsequent to the setting of cookies, particularly where it involves appending or matching any other data to an explicit profile or an identifier involves the processing of personal data. This processing is subject to the provisions of the GDPR, including the provisions relating to data subject rights.
- The DPC came across examples in the course of this sweep, and has come across further examples since, of CMP settings with non-exempt cookies set by default to on, with the choice of the user to reject these cookies by means of unchecking the box not respected. Such issues will be a priority for enforcement.

Enforcement

While this sweep was conducted on just a small number of controllers, it has highlighted a significant landscape of tracking of users of Irish-based websites.

Bringing controllers into compliance with the current ePrivacy Regulations will be a significant challenge, in particular due to the vast, worldwide nature of the processing operations underlying the adtech sector. There may also be a general resistance among controllers to changing their user interfaces where this involves cost and/or the introduction of what they might tend to see as 'friction' in the design process. The possibility of inducing 'consent fatigue' among users faced with having to choose their settings on each visit to a website was also raised by some controllers during the sweep and there is indeed a balance to be struck between the provision of adequate information for users and design that is minimally obtrusive to the user experience.

There is a danger that, even where they engage positively with the DPC, that controllers will make cosmetic changes to their websites without any real transparency for data subjects about how data relating to them is being processed, or without any real means for data subjects to exercise their rights under the GDPR.

However, as a start, we would consider it a significant achievement to bring these 38 controllers and others into compliance as regards the consent requirements and the transparency requirements around their use of cookies and other tracking technologies.

Any further engagement with controllers on foot of this sweep must also emphasise their comprehensive obligations to provide transparent information about their processing of personal data, including special category personal data, under the GDPR where they are processing personal data linked to their use of cookies and other tracking technologies.

As noted above, one controller in this sweep appeared to be specifically combining data derived from cookies and trackers with loyalty card information, while a banking organisation also combined information entered into loan calculation forms with information derived from cookies. Controllers must be able to demonstrate their lawful bases for all processing of personal data, including where that data is derived from cookies and other tracking technologies. In addition, controllers must provide transparent information to data subjects about such processing, in line with their obligations under the GDPR and the Data Protection Act 2018.

Where controllers fail to voluntarily make changes to their user interfaces and/or their processing, the DPC has enforcement options available under both the ePrivacy Regulations and the GDPR and will, where necessary, examine the most appropriate enforcement options in order to bring controllers into compliance with the law.

Tools available to us in the GDPR and the Data Protection Act 2018 include the use of inquiries (with or without an investigation), inspections or audits to examine all aspects of a controller's processing of personal data. This may be a particularly effective option should further action be considered necessary, for example, in relation to health-related websites or other sites where controllers link data from cookies to an explicit profile or identifier.

This would include an examination of a controller's compliance with its transparency and accountability obligations, its obligations to maintain a record of processing activities, its general obligations with regard to data subject rights under the GDPR, its security obligations under Article 32 of the GDPR, and its controller-processor contracts.

ENDS

6 April 2020

Annex: letter to controllers commencing cookies sweep on 15 August 2019

15 August 2019

Re: Notification of sweep survey regarding cookies

Dear

The Data Protection Commission is undertaking an examination of the use of cookies on a selection of websites and _____ is one of those we have chosen for examination.

The purpose of this sweep survey is to request information to allow us examine the deployment of cookies and similar technologies by data controllers and to establish how organisations are complying with the law.

To this end, and in accordance with Article 31 of the General Data Protection Regulation, we write to request your cooperation with the DPC and your participation in the sweep.

The purpose of the law on cookies is to protect the confidentiality of communications, which is guaranteed in accordance with international instruments relating to human rights, in particular the European Convention for the Protection of Human Rights and Fundamental Freedoms.

On 1 July 2011 Statutory Instrument No. 336 of 2011 European Communities (Electronic Communications Networks and Services)(Privacy and Electronic Communications) Regulations 2011 (**"the ePrivacy Regulations**) came into law in Ireland. The legislation, including Regulations 5(3), 5(4) and 5(5), is outlined in **Appendix II.**

The ePrivacy Regulations give effect to Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 as amended by Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 and Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009.

These rules apply to certain types of data processing, including the use of cookies and similar technologies, and they are now read together with the General Data Protection Regulation and the Data Protection Act 2018.

Note that the standard of consent required by the GDPR is higher than that under previous data protection legislation and requires that consent must be a clear, affirmative act, freely given, specific, informed, and unambiguous.

Our expectation is that you will be able to demonstrate the action your organisation has taken to comply with the rules for cookies, particularly in light of this higher standard of consent now applicable under the GDPR. We also expect that you demonstrate how your organisation is meeting its responsibilities under Article 24 of the GDPR, which provides that data controllers shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with that regulation.

I attach in **Appendix I** a list of questions to which we require you to respond, so that we may further assess your organisation's compliance.

It is also open to you to provide us with any additional information you believe is relevant regarding your organisation's compliance with the law.

I attach for your information a copy of the DPC's Guidance on Cookies and Similar Technologies.

The DPC's aim is to ensure that organisations comply with the law. In cases where organisations refuse or fail to comply voluntarily, the DPC has enforcement powers available to it.

Please respond to this letter by Thursday 26 September 2019, preferably by email to siu@dataprotection.ie

_____

Special Investigations Unit

APPENDIX I

Please provide responses to the following questions. If appropriate, please include tables and/or process maps outlining the customer journey and consent management processes used on your website in relation to cookies.

Please confirm the full name and address of the data controller for the website _____. Confirm whether this website uses cookies.

1. List, in a table where necessary, the names, types, functions, security, origin and lifespans of all cookies deployed when a user visits _____, either as a first-time visitor, when a user is redirected to your site from another site, or as a return visitor. This list should indicate for each cookie whether it is a first-party or third-party cookie and which domain is its host. Indicate whether a cookie is determined to be "strictly necessary" or optional, and if so how this determination is made.
2. List all the third parties whose cookies or assets, including 'like' buttons, plugins, pixels, beacons, audience measurement tools or otherwise that are deployed on your website. Describe the purpose of each of these and how they are used and processed by your organisation, including for analytics.
3. Where third party cookies or assets are deployed describe whether the data controller of the website is a joint controller with such third parties, or otherwise.
4. Please describe how you ensure users are aware of any third party activity, such as analytics or advertising, taking place on your website, and what information you are providing to users about how to control that third-party activity via their browser.
5. Please provide screenshots of the information presented to users in relation to cookies when they visit your website. Include, where necessary, all interstitials, banners, notices, pop-ups and other means used to draw a user's attention to the use of cookies.
6. Demonstrate in your response how a user's consent is captured prior to the storage of information, or the gaining of access to information already stored, on the user's terminal equipment.
    a. Provide details of how this consent meets General Data Protection Regulation (GDPR) requirements for precise, unambiguous and affirmative consent, in particular how consent is recorded and can be demonstrated by the data controller, as per Article 7(1), and how it can be withdrawn as per Article 7(3)
    b. Provide details of any privacy controls implemented, including information on sliders, buttons, UX, push notices or any other methods

used to alert users to the use of cookies and to enable them to make choices about the use of such technologies. Describe the intended functionality of each control.

   c. Confirm whether storage or access to information on a user's terminal equipment occurs before or after consent is obtained and recorded.
   d. Describe how a user may, subsequent to an initial visit and interaction with any consent mechanism, vary their initial consent choices.
   e. Where applicable, describe the circumstances and reason why consent may again be sought from a user who has initially refused consent
   f. Describe any differences in the consent capture mechanism when accessed from a mobile device, compared to a desktop computer.
   g. Describe how your cookies and consent mechanism interact with any installed "cookie blocker", or "ad blocker" technology, including detection of such.
   h. If any such "cookie blocker" or "ad blocker" is detected, please describe if, and how, this affects the user's ability to browse and view content on your website.

7. Does the user have any control over the cookies which could be stored on their terminal device?
   a. If user controls exist, please describe the default settings for controls in the cookie consent mechanism used for your website.
   b. For each cookie that is enabled by default and cannot be turned off via any user controls, please outline
      i. The name of each cookie that falls into this category
      ii. The reason for no controls being in place to prevent storage of the cookie.
8. Demonstrate how the information provided to subscribers or users is clear and comprehensive, prominently displayed and that it includes, without limitation, the purposes of the processing.
9. Please provide a full electronic copy of your cookies notice and all information available on your website in relation to the use of cookies. Include, where possible, a screenshot of any headers or footers containing information about cookies, and the URLs where this information may be found. You should be able to demonstrate that this information is both prominently displayed and easily accessible.
10. Please indicate if users are redirected to any third-party sites in order to access information about third-party cookies placed on terminal equipment when they visit your site. Please provide the URLs or domain names.

11. Please provide a copy of your privacy policy or notices made available to users of your website and indicate how and where on your site this information is displayed.
12. If your organisation has not achieved compliance with the ePrivacy Regulations, please explain why this is the case, with a clear timescale for when compliance will be achieved, and specific details of what work is being done to make that happen.
13. Please provide any additional or supplemental information that you feel may aid your response to this sweep questionnaire that may not have been covered by any previous questions.

APPENDIX II

Legislation on cookies

Article 5(3) of Directive 2002/58 (as amended by Directive 2009/136/EC):

> *"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. 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."*

Regulation 5(3) of the ePrivacy Regulations (S.I. No. 336/2011):

> *"A person shall not use an electronic communications network to store information, or to gain access to information already stored in the terminal equipment of a subscriber or user, unless*
>
> *(a) the subscriber or user has given his or her consent to that use, and*
>
> *(b) the subscriber or user has been provided with clear and comprehensive information in accordance with the Data Protection Acts which—*
>
> *(i) is both prominently displayed and easily accessible, and*
>
> *(ii) includes, without limitation, the purposes of the processing of the information.*

Regulation 5(4):

> *"For the purpose of paragraph (3), the methods of providing information and giving consent should be as user-friendly as possible. Where it is technically possible and effective, having regard to the relevant provisions of the Data Protection Acts, the user's consent to the storing of information or to gaining access to information already stored may be given by the use of appropriate browser settings or other technological application by means of which the user can be considered to have given his or her consent."*

Regulation 5(5):

> *"Paragraph (3) does not prevent any technical storage of, or access to, information for the sole purpose of carrying out the transmission of a communication over an electronic communications network or which is strictly necessary in order to provide an information society service explicitly requested by the subscriber or user."*

Recital 24 of the ePrivacy Directive 2002/58 clarifies the obligation to ensure the confidentiality of communications:

> *"Terminal equipment of users of electronic communications networks and any information stored on such equipment are part of the private sphere of the users requiring protection under the European Convention for the Protection of Human Rights and Fundamental Freedoms*.
>
> *So-called spyware, web bugs, hidden identifiers and other similar devices can enter the user's terminal without their knowledge in order to gain access to information, to store hidden information or to trace the activities of the user and may seriously intrude upon the privacy of these users. The use of such devices should be allowed only for legitimate purposes, with the knowledge of the users concerned."*

Definition of consent under Article 4(11) of the General Data Protection Regulation:

> *"'consent' of the data subject means any 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"*

Article 24 of the General Data Protection Regulation - responsibility of the controller:

> **24(1)** *"Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. ₂Those measures shall be reviewed and updated where necessary."*
>
> **24(2)** "*Where proportionate in relation to processing activities, the measures referred to in paragraph 1 shall include the implementation of appropriate data protection policies by the controller."*

---

[i] Directive 2002/58/EC of the European Parliament and the Council of 12 July 2002: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32002L0058&from=EN

[ii] Article 29 Working Party Opinion on online behavioural advertising 22 June 2010, page 13 (PDF): https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp171_en.pdf

[iii] Opinion 2/2010 on online behavioural advertising https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp171_en.pdf (PDF)

[iv] Article 29 Working Party Opinion 04/2012 on Cookie Consent Exemption, page 5 (PDF): https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp194_en.pdf

[v] *How top health websites are sharing sensitive data with advertisers*, Financial Times, 13 November 2019. (Link may be paywalled: https://www.ft.com/content/0fbf4d8e-022b-11ea-be59-e49b2a136b8d)