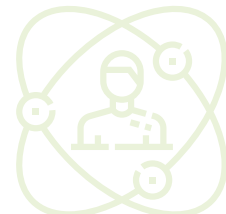




Cookie Benchmark study

April 2020



Contents

Executive summary	4
Introduction	5
Regulatory factsheet	6
The importance of gaining and maintaining trust	7
Cookies settings in practice	8
<i>Transparency and cookie notifications</i>	9
<i>Cookie consent management</i>	10
<i>Nudging users to accept cookies</i>	11
Cookie and website security	12
Purposes for processing cookies	14
Cookies by third parties	15
Cookie compliance insights from a country-perspective	16
Insights on the actions of authorities	18
Four cookie cases explained	20
Performing a check of your own website: a Do-It-Yourself (DIY) guide	22
Creating a user-centric cookie experience	24
Contacts	26
Annex – Research methodology	28
Overview of the websites reviewed	29

Executive summary

The General Data Protection Regulation (“GDPR”) and the ePrivacy Directive set the rules for cookie practices of organisations. Have these regulations had the impact desired by regulators? Do they enhance individuals’ privacy?

Deloitte conducted research using a sample of 167 websites across 12 countries within the European Union to gain insight into the way organisations deploy cookies. The websites examined are distributed across six industries, which allowed us to analyse patterns across different industries. In conducting this study, we focused on factors around transparency, consent, security and cookies placed.

Cookies Consent Management
Following the recent regulatory shift, cookie notifications are becoming crucial for enhancing privacy. Most organisations seem to understand the value of transparency as their websites contain an explanatory text on cookies. However, improvements are needed to allow users to give their valid consent.

The importance of cookie and website security
With regard to cookies, privacy and website security are two inseparable components. Securing session cookies is paramount to achieve this bi-dimensional target. Our research revealed that only 4% of all websites reviewed use fully secure headers.

Purposes for processing cookies
Cookies can be categorised as “strictly necessary”, “functional”, “performance” and “tracking and advertising” cookies. The various purposes have different consent requirements. 55% of websites’ consent tools analysed in this benchmark study did not offer the possibility to pro-actively tailor users’ cookie consent settings.

Third party cookies
The most commonly found cookies across all websites reviewed come from third party services. These have various purposes, ranging from basic website functionality to advertisements. Whilst useful due to their ease of use, these services can come with additional data protection requirements, as data might be shared with these third parties.

Insights from a country-perspective
Looking at trends throughout different countries, we noted how notifications have been homogeneously implemented in the form of banners across the board, with the exception of Norway. Belgium, Greece and the Netherlands have the highest number of websites with adjustable cookie settings.

Insights on the actions of authorities
Certain national supervisory authorities are publishing guidelines on the use of cookies and are actively investigating cookie practices adopted by organisations. Yet, it is still uncertain how the current framework, set out by the authorities, will be affected after the introduction of the ePrivacy Regulation.

Gaining and maintaining trust
The perception of an organisation can be largely influenced by the way it handles its cookies. Implementing user-centric methods to manage cookies and adopting sophisticated tools to gather consent can be important unique selling points and can grant organisations a relevant competitive advantage.

Performing a website check
With all the information provided in this report you might wonder about the status of your organisation’s website. By following the step-by-step guidance, included in this report, you can manually check whether the website has implemented certain cookie requirements.

Introduction

This Benchmark Report provides key information about pressing questions relating to the current and future regulatory framework concerning cookies. The report addresses the main insights on how cookie compliance is tackled in various industries and countries within the European Economic Area (European Union plus Norway, Liechtenstein and Iceland).

About the research

The Cookie Benchmark study is based on an analysis of 167 websites of organisations in six industries: Technology, Media and Communications (TMC); Consumers (Cons.); Energy Resources & Industrials (ERI); Financial Services (FS); Life Sciences and Healthcare (LSHC) and Government and Public Services (GPS). The websites were surveyed between October and November of 2019.

The research was conducted through a collaborative effort between multiple Deloitte firms across North and South Europe. It included websites across 12 countries to get a view of the compliance level of organisations’ websites when it comes to cookie practices. The countries surveyed were Belgium, Denmark, Finland, Greece, Iceland, Ireland, Italy, the Netherlands, Norway, Sweden, Switzerland and the UK.



Regulatory factsheet

In the Union¹, cookies are regulated by two main instruments: the ePrivacy Directive, which, amongst other things, requires consent for the placement of certain cookies, and the GDPR, that defines consent. The future ePrivacy Regulation may further harmonise the legal framework and add new requirements.



1. The ePrivacy Directive

The ePrivacy Directive regulates the privacy, confidentiality, and security of “electronic communications”, which includes cookies.

More specifically, the ePrivacy Directive states that marketing and advertising cookies can only be placed if the user has given consent. Functional and necessary cookies are exempt from the requirement to obtain consent. The ePrivacy Directive uses the GDPR’s definition of consent.



3. The GDPR

The General Data Protection Regulation regulates the protection of personal data of individuals in the Union. It applies to all personal data, regardless of its technical form (including cookies).

The GDPR’s consent requirements are key components for cookie compliance: consent to the placement of cookies needs to be freely given, specific, informed and unambiguous, as well as expressing the data subject’s wishes by a clear affirmative action.

A legal basis is not only required for the placement of cookies: organisations also need a separate legal basis for the subsequent processing of personal data which is obtained through tracking technologies.



Types of Cookies

On the basis of this regulatory framework, cookies can be categorised into four different groups.

- 1. Strictly necessary cookies.** These cookies are essential for the sole purpose of providing the service requested, such as holding items in your online shopping cart.
- 2. Performance cookies.** These cookies collect information on how visitors use a website, such as page visits and page load speed. With solely this information, a visitor cannot be identified.
- 3. Functionality cookies.** These cookies allow a website to remember choices visitors make, such as user name and language, and provide enhanced, personalised results.
- 4. Targeting or advertising cookies.** These cookies are used to deliver adverts that are more relevant to the user as they are based on their interests. They can be set even if the site itself does not display advertising. These cookies often are third party cookies.

This categorisation is relevant because not all cookies require consent. For more information on this, please refer to [page 8](#)



2. The ePrivacy Regulation

The draft ePrivacy Regulation aims to update the existing legal framework and will replace the ePrivacy Directive if and when this regulation is adopted. It envisages an expansion of the definition of electronic communications and further harmonisation of the rules throughout the Union.

On the subject of cookies, it is likely that the future ePrivacy Regulation will specify rules on expressing consent via browser settings, and clarify the rules with regard to the use of legitimate interest as a legal basis.



4. The rules in practice

With the ePrivacy Directive currently undergoing a legislative update, and the GDPR having been enforceable for just under two years, it is important to highlight that the regulatory framework applicable to cookies is evolving. Courts and supervisory authorities are adding clarifications and interpretations to existing rules and best practices are being formulated. Furthermore, the ePrivacy Regulation will add new, most likely stricter, conditions to the placement of cookies.

The importance of gaining and maintaining trust

Six months after the GDPR came into force, we published a “GDPR Six Months On” report in which the attitudes towards privacy of both consumers and organisations were surveyed and analysed. We found that the adherence to cookie requirements constitutes a unique selling point. Consumer trust is inextricably linked to the way websites handle online privacy, with transparency and user-centric cookie management being the cornerstones of this evolving landscape.

Our report: *“GDPR Six Months On: A new era for privacy”*



1. Consumer trust and ethics

The majority of organisations regard increasing consumer trust to be a driver to achieve regulatory compliance. In fact, the perception of an organisation can largely be influenced by the way it handles consumers’ privacy. Moreover, properly disclosing data handling criteria has become a prime factor in determining an organisation’s ethical dimension. This is particularly relevant since 69% of consumers find an organisations’ ethical reputation to be the main factor constituting their degree of trust towards that organisation. Interestingly we have noticed that organisations still have a long way to go in understanding the value of transparency when gathering users’ consent. There is a somewhat established tendency to use shortcuts or nudge website users towards accepting cookies without creating a trustworthy relation with the users. We discuss this issue in detail in a dedicated section of this report: [“Nudging users towards accepting cookies”](#)

69% of respondents feel that an organisation’s reputation plays an important factor in their level of trust in that organisation



2. Cookie management practices influence consumer trust

A growing percentage of users is aware of their privacy rights and claims to be active in managing cookie settings when visiting a website. The findings of Deloitte’s 2018 “GDPR Six Months On” report revealed the link between users’ level of trust in an organisation and the cookie management practices of that organisation. We also observed that the vast majority of users consider an excessive use of cookies to be a concern for them. In light of the foregoing, organisations may want to provide users with tools to tailor their privacy disclosure. The report also shows that 70% of consumers reported to be uncomfortable with tailored advertising. Therefore, it might be advantageous for organisations to clearly communicate user-centric measures such as keeping the amount of personal data collected or stored to a minimum.

65% of our respondents agreed that excessive use of cookies raises a privacy concern for them



3. Cookies management as a business opportunity

Consent Management Platforms (CMPs), have developed interactive tools to tailor users’ consent through opt-in or opt-out functions. Cookie setting tools, for example, can allow users to actively opt in to “non-strictly-necessary” cookies, putting them in charge of the data they share. These tools do not only give organisations the chance to secure consumers’ trust, but also to interact with them from a commercial perspective. Notably, 60% of users are willing to share more data in exchange for personalised benefits and discounts. Organisations therefore can restructure their privacy strategies around the concept that personal data are not just a matter of ethics, but are increasingly becoming a business opportunity.

60% of consumers are willing to share more data to receive personalised benefits and discounts

¹ European Economic Area (European Union plus Norway, Liechtenstein and Iceland), referred to as “the Union”.

Cookies settings in practice

In principle, it is forbidden to place tracking technologies, such as cookies, onto an end-users' device. However, this is allowed when necessary for the communication, the service, analytics, security updates, or when the end-user has given consent.

Good practice example, based on the cookie banner of the ICO (ico.org.uk) on 23 March 2020.

Our use of cookies
We use necessary cookies to make our site work. We'd also like to set optional performance cookies to help us improve it. We won't set optional cookies unless you enable them. Using this tool will set a cookie on your device to remember your preferences.

For more detailed information about the cookies we use, refer to our Cookies page.

Strictly necessary cookies
Strictly necessary cookies enable core functionality such as security, network management, and accessibility. You may disable these by changing your browser settings, but this may affect how the website functions.

Performance cookies Off
We'd like to set Google Analytics cookies to help us improve our website by collecting and reporting information on how you use it. The cookies collect information in a way that does not directly identify the user.

Save and close

- Not all cookies are treated the same**
Cookies can be categorised into four different groups (for more information, go to the section [regulatory factsheet](#)). Targeting or advertising cookies always require consent of the user, while functional cookies generally require consent. However, you do not need consent for strictly necessary cookies as these are essential for providing the service that the user asks for. Performance cookies do not require consent if a visitor cannot be identified by them. In the good practice example we see that consent is requested for performance cookies. As the website is not placing functional or advertising cookies.
- Consent must be informed**
Organisations must inform users about data collection activities in a clear and comprehensive manner. As a minimum, a cookie notice must explain the purpose for the installation of cookies and state which actions will indicate consent. It must be noted that it is good practice to provide users with information about cookies, even if consent is not required.
- Pre-ticked boxes do not equal consent**
Consent must be obtained in accordance with the GDPR requirements. This requires a clear affirmative act, that is freely given, specific, informed and an unambiguous indication of the users' wishes. For example, boxes that are already checked do not count as an unambiguous affirmative act. A clear on/off-button is good practice, if the button is by default switched off.
- Users are allowed to change their minds**
A user must be able to withdraw consent at any time. In addition, it must be as easy to withdraw as to give consent. For cookies, this generally means that users should be able to withdraw consent through the same action as when they gave consent.

As a good practices, a cookie control centre is constantly present during the browsing session to enable the user to easily change the cookie settings.

Transparency and cookie notifications

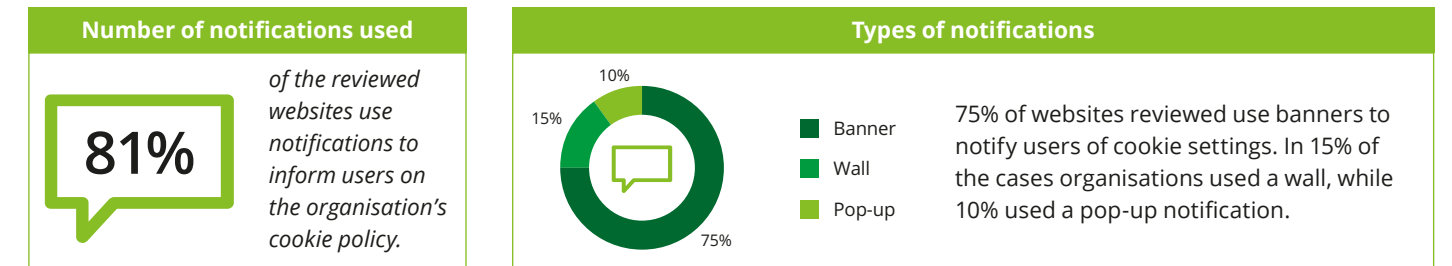
How do organisations provide transparency and notify users of cookie policies adopted?

Transparency

Transparency is a key principle under the GDPR. Organisations inform individuals about their online cookie practices through cookie pop-ups, banners or walls for this purpose.



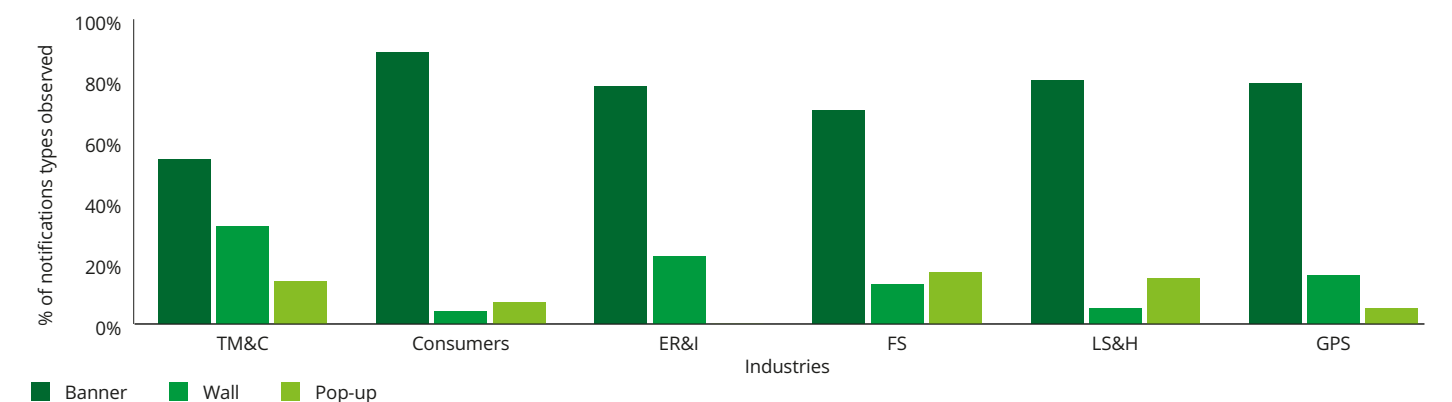
A cookie pop-up is a small window that suddenly appears in the foreground of the visual interface. A cookie banner is somewhat different, since it does not suddenly appear but remains consistently visible at the top or at the bottom of the webpage. While both pop-ups and banners allow visitors to access the initial webpage before consenting to cookies, walls are windows that do not permit access to the webpage content until consent is given. We noticed that most websites reviewed notified visitors of the use of cookies and that most often these notifications take the form of banners.



Notification trends across industries

Throughout the 6 industries that we looked at, we noticed some dissimilarities regarding the different kinds of notifications used on websites. While the Technology, Media and Communications industry registered the most significant variance in the typology of notification tools, organisations in the Consumer industry mainly utilise banners to inform the audience on their cookie policy. Notably, organisations in Energy, Resources and Industrials use banners and walls but do not rely on pop-ups to notify visitors of their cookie policies.

Notification types per industry



Cookie consent management

Websites manage consent through different mechanisms, providing users with different opportunities to tailor cookie preferences.

Different types of cookie consent management mechanisms

Not all cookie notifications present users with the same cookie management opportunities. We have identified three main consent management practices: "opt-in", "opt-out" and "no consent option available":



Users can "opt-in" to certain categories of cookies which were not yet in use. Consent is given by the selection of which cookies can be activated.



Alternatively, we see that the reverse procedure is also used to obtain consent: cookies are placed by default. Users can opt-out of the categories of cookies which they want to decline.



Other consent banners simply inform the user that by navigating the website or "closing this banner", the user accepts the placement of cookies. We categorised this option as "no consent option available".

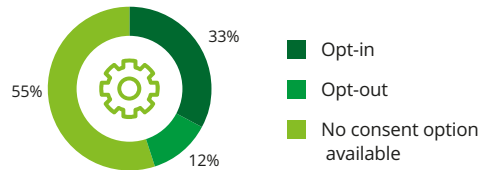
Consent Management Platforms

Consent Management Platforms (CMPs) are third party providers that supply websites with the technical capabilities to inform users on cookie settings and to gather consent. These platforms allow websites to automate the cookie management process, making it easier for organisations to be GDPR compliant.

The majority of websites does not validly obtain consent

Cookie consent management

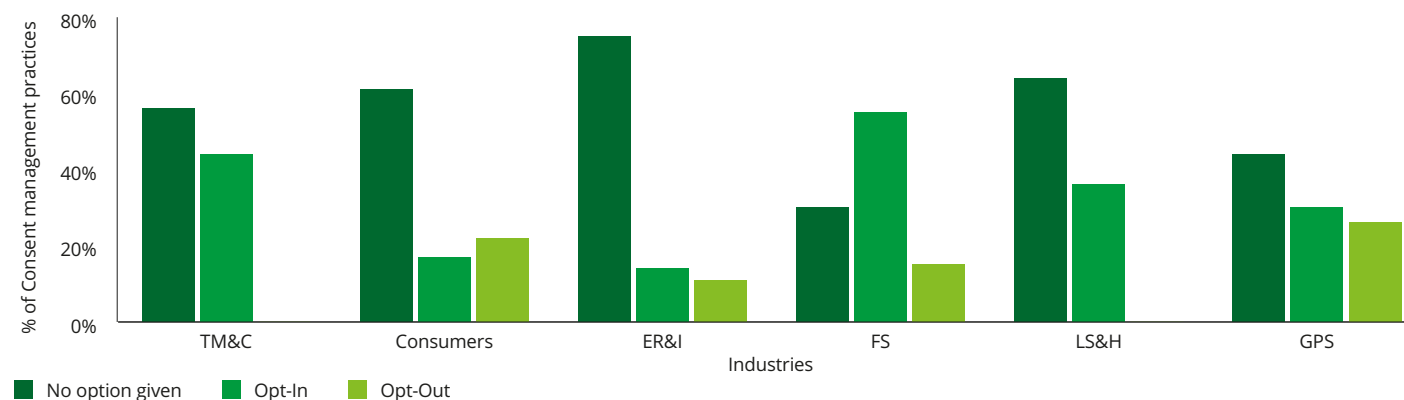
55% of websites' consent tools analysed in this benchmark study did not offer the possibility to pro-actively tailor users' cookie consent settings. The remaining 45% of consent tools researched allowed either to opt-in (33%) or to opt-out (12%) to certain categories of cookies.



Financial services industry sets the example regarding consent management

In our research for this benchmark study, we observed that cookie management mechanisms vary among the industry groups. In the Financial Services industry, 55% of the researched websites provide the possibility to opt-in to certain categories of cookies. For the other industries, most websites do not display proactive cookie management solutions. 75% of the websites in the Energy Resources & Industrials industry place cookies without obtaining the required consent. Additionally, websites within this industry have the lowest "opt-in" percentage compared to the other industries.

Consent management per industry



Nudging users to accept cookies

How websites use eye-catching cookie banners to obtain consent

Nudging based on visual triggers

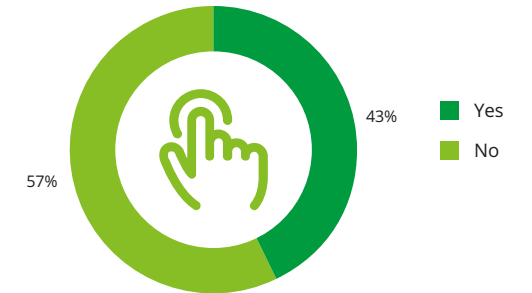
As the GDPR made it compulsory for organisations to inform users and obtain their consent prior to placing cookies, websites have adopted creative visuals to invite visitors to provide their consent. A typical example of this phenomenon is the use of banners featuring big green buttons for the "accept all cookies" function and a smaller faded-grey equivalents for the "decline cookies" option. Another recurring practice is that users need to go to great lengths to decline cookies by clicking through a series of settings, while the option to accept cookies is directly available.

Overall use of nudging techniques

In conducting this benchmark study we tested the use of nudging techniques in all websites that enabled users to share cookie preferences by opting in or out.

The following features were used to determine whether users were nudged to accept cookies: strategic use of font size, colour and level of complexity to accept and decline cookies.

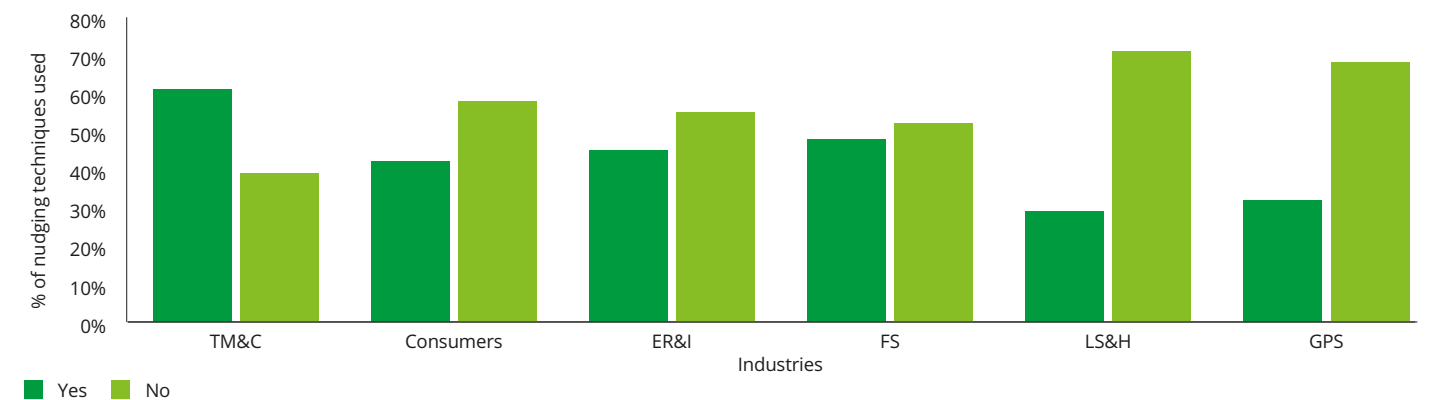
Notably, 43% of the websites in scope were deemed to nudge individuals towards accepting all cookies.



Users are nudged to give consent most often by organisations in Technology, Media and Communication industry

Organisations have different approaches to gathering consent, and some industry groups have a greater tendency to use eye-catching consent buttons. 61% of cookie notifications in the Technology, Media and Communications industry featured attractive fonts and colours to nudge visitors towards accepting all cookies used on the website. The websites reviewed in the Life Science & Healthcare and Government and Public Services industries only use nudging techniques in respectively 29 and 32 percent of the reviewed websites.

Nudging practices per industry

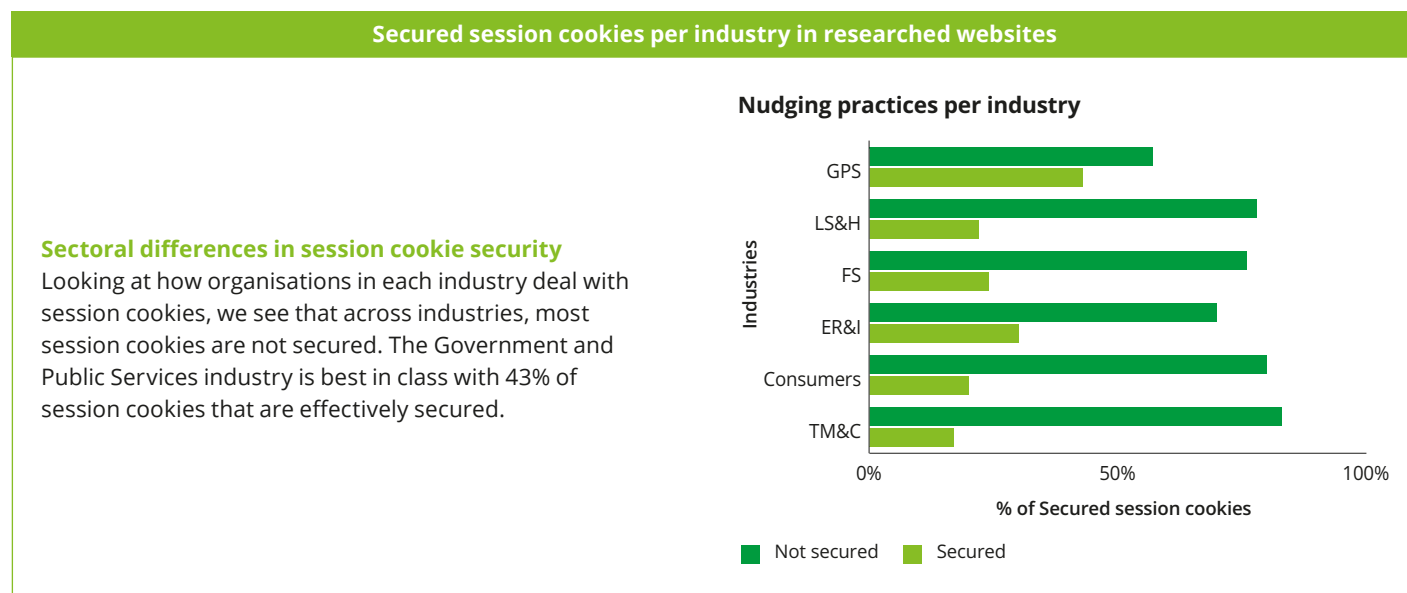
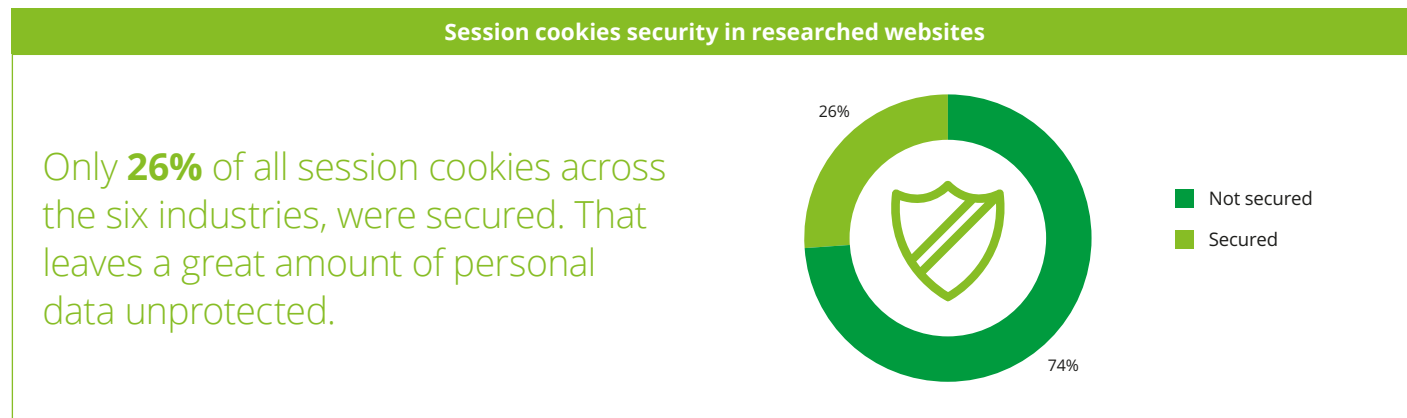


Cookie and website security

Do organisations adequately protect personal data on their website?

The importance of secured session cookies

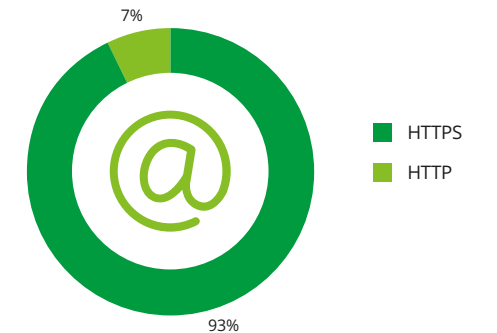
Website security is an important factor for protecting users' online privacy. It preserves the confidentiality and integrity of processed data and helps protect against malicious activities and theft of information. In particular, securing session cookies is pivotal for data protection. Session cookies contain a unique identifier which allow a website to enable basic functionality (such as a shopping cart) by tracking the behaviour of a user across the website pages. If this information is sent via unencrypted traffic, malicious actors can recreate the cookie and impersonate the user by sending the same information to the website. This is called "session hijacking" which can be avoided by ensuring traffic encryption.



Security of communications protocols in researched websites

Encrypted communication through HTTPS

In order to maintain good security, websites need to prevent communications between the browser and the web server taking place without using encryption. This step is crucial to prevent malicious actors from intercepting information sent in plain text. Protecting against man-in-the-middle, eavesdropping and tampering attacks, HTTPS does as much for security as for privacy, ensuring authentication, integrity and confidentiality standards during data exchanges.



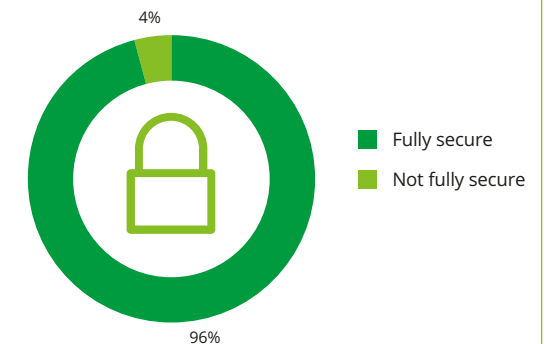
93% of the researched websites use secure encryption protocols (using SSL/TLS), while **7%** of websites is accessible via unencrypted HTTP protocols

Security of communications protocols in researched websites

Website security headers for secure communication

Website security headers are at the core of secure communication exchanges and represent an additional instrument to protect information. To assess the security level of request-response cycles we looked into four different headers:

1. "Content Security Policy" headers provide the possibility to administer the resources that users of the website are allowed to access and load. This security layer helps reduce the risk of code injections and cross-site scripting attacks.
2. "Cache Control" headers specify caching policies in use in both user requests and server responses. This allows to determine of which website information is stored on the user's web browser, and for how long.
3. "Referrer Policy" headers control the disclosure to the destination website of address information of the website where the request originated. Destination websites can use information on the origin of requests to assemble metrics and track user traffic patterns. This information is considered personal data. Transmitting this information through the Referrer Policy header adds to the security of this information.
4. "Strict Transport Security" headers ensure that all communication circulates via HTTPS. This measure is particularly useful against protocol downgrade attacks and cookie hijacking: when a website uses secure encryption protocols, there is still a window of opportunity for hackers to intercept traffic when switching from HTTP to HTTPS. This header disregards script's request to load any resource over HTTP.



Only **4%** of all websites reviewed use fully secure headers, including Content Control, Cache Control, Strict Transport and Referrer Policies

Purposes for processing cookies

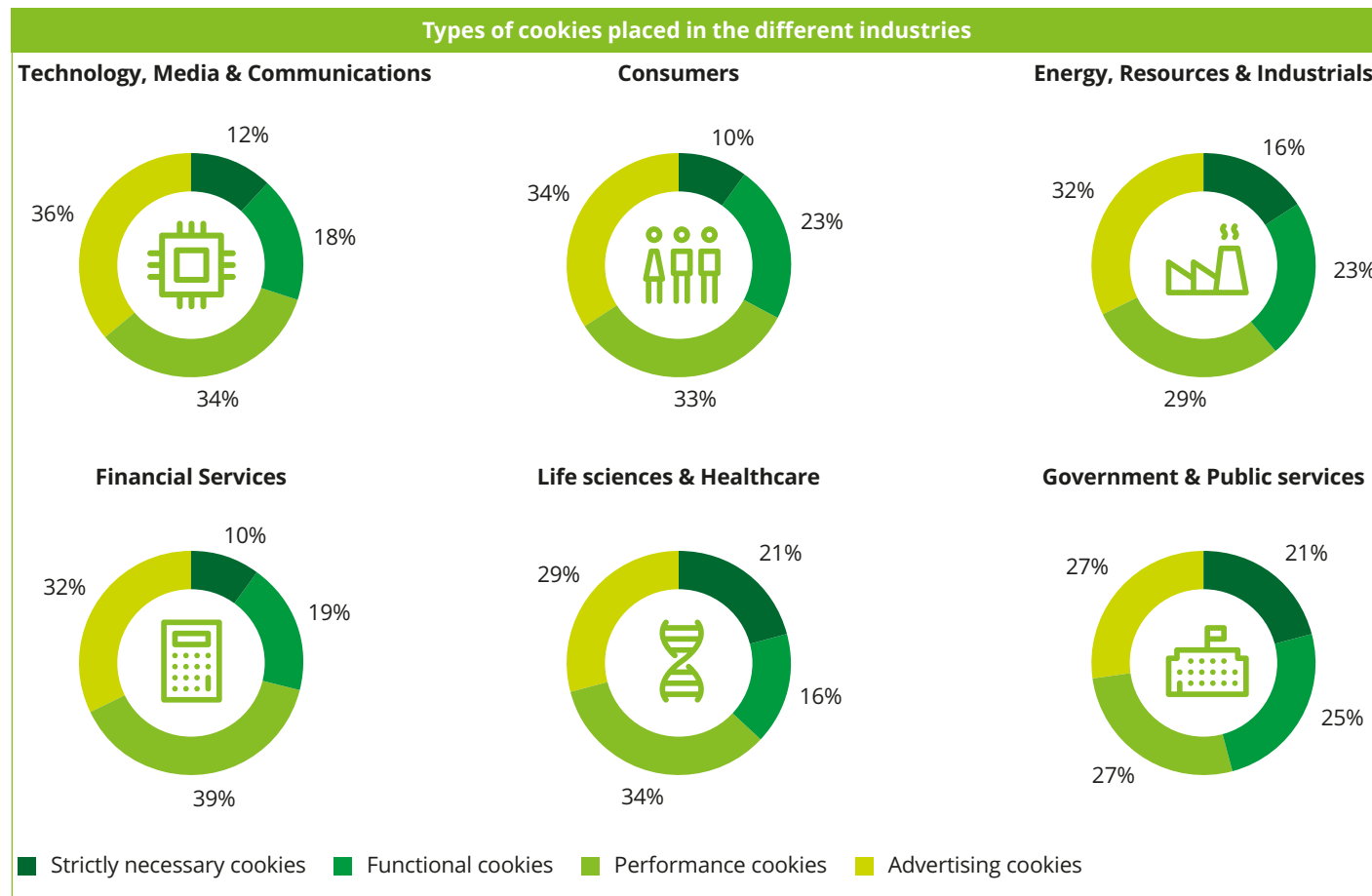
An overview of the types of cookies placed

Cookies can serve a variety of purposes. Website owners can use them to enhance website functionalities, to monitor how users use a website, but also to identify users and to offer them tailored ads. Varying legal requirements are linked to these different types of cookies. This is further explained in the section [“cookies and consent”](#).

Cookie distribution

In total, 2598 cookies were placed across the 167 websites researched. 12% of the cookies placed were strictly necessary cookies. 18% of the cookies were functional, 28% were performance, and 27% were tracking and advertising cookies. The remaining 15% could not be identified. These unidentified cookies were left out of the pie charts below for greater legibility.

27% of the cookies placed across the researched websites were tracking and advertising cookies.

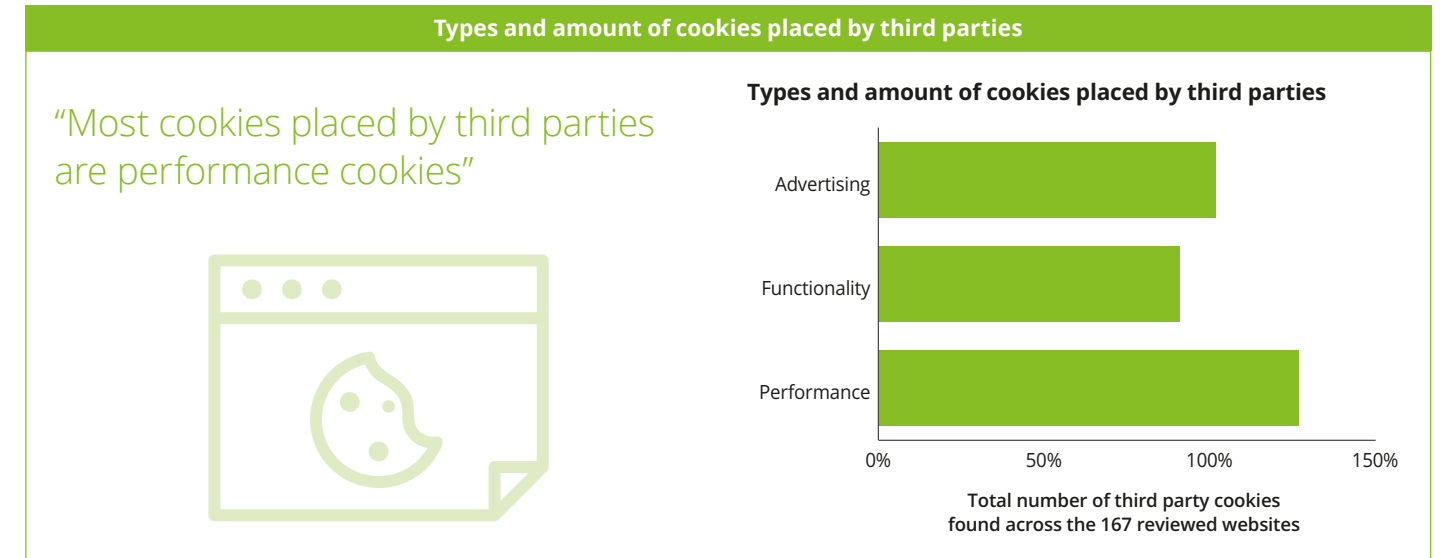


Reviewed websites of organisations in Technology, Media & Communications industry place most tracking and advertising cookies

The different types of cookies used within industries exhibit a similar pattern. In all, we can see that performance, and tracking and advertising cookies are by far the most prevalent cookies.

Cookies by third parties

A closer look at the most commonly cookies placed



Third party services come in many forms and functions. Some are used to give the website owner an easy way to manage website infrastructure. Others are part of analytics packages which give owners the ability to monitor how their website is being used. A third type of services allows for targeted advertising and tracking of users across sites, usually in return for ad-revenue.

Third parties placing tracking and advertisement cookies allow for the identification of users across websites by assigning them a unique ID that is persistent. This ID links to the user profiles which are created by tracking the online behaviour of the individual. These profiles are interesting for organisations as this allows for targeted advertising, the revenue of which the website owner gets a part after a user clicks on an advertisement.

Performance suites provide tools which allow website owners to monitor website usage, so organisations can see the amount of new and return visitors, how visitors browse their websites and which links are clicked on.

The suites offering functionality cookies enable a website owner to present their visitor with a functioning website. The suite is aimed at improving the user experience and protecting the website owner by managing website traffic, scanning for bots, and blocking malicious users based on an IP check.

Explicit consent and specific notification of users

Website owners use various third party services to outsource the management of cookie settings on their website. Whilst this is useful from a business perspective, it can come with additional privacy requirements. Following best practice, website owners should make sure that other than strictly necessary and functionality cookies are only placed after the user has been informed about the cookies placed and has actively opted-in to this.

Cookie compliance insights from a country-perspective

The research conducted contains an analysis of the use of cookies within 12 different countries. The country specific insights are based on our research of multiple websites, covering six industries across the countries. Here we discuss the particularities and differences we found per country.

Cookie notifications

Our research found that most of the reviewed websites use cookie notifications, predominantly in the form of a banner. Norway could be considered the odd one out, where 5 out of 12 websites did not have any cookie notification whatsoever.

Opting in to cookies

We inspected how websites collect cookies: through opt-in, opt-out or by not allowing to decline cookies. It is interesting to see that in most countries, the cookie notifications did not allow the user to decline cookies: in 25,7% of the websites we reviewed, it is possible to opt-in to cookies. Only in Belgium (46%), Finland (40%) and the Netherlands (40%) the results were higher for the opt-in process.


Adjusting cookie settings

We examined whether the cookie notifications provide users with the option to adjust the settings directly from either the pop-up, banner or wall. Out of 167 websites, only 27 provided users with an explicit option to change the settings directly through the cookie management tool. From these 27 websites, Belgium, Greece and the Netherlands have the highest number of websites with adjustable cookie settings. Overall, 84% of the 167 websites reviewed do not allow the user to change the cookie settings directly from the cookie notification.

Transparency

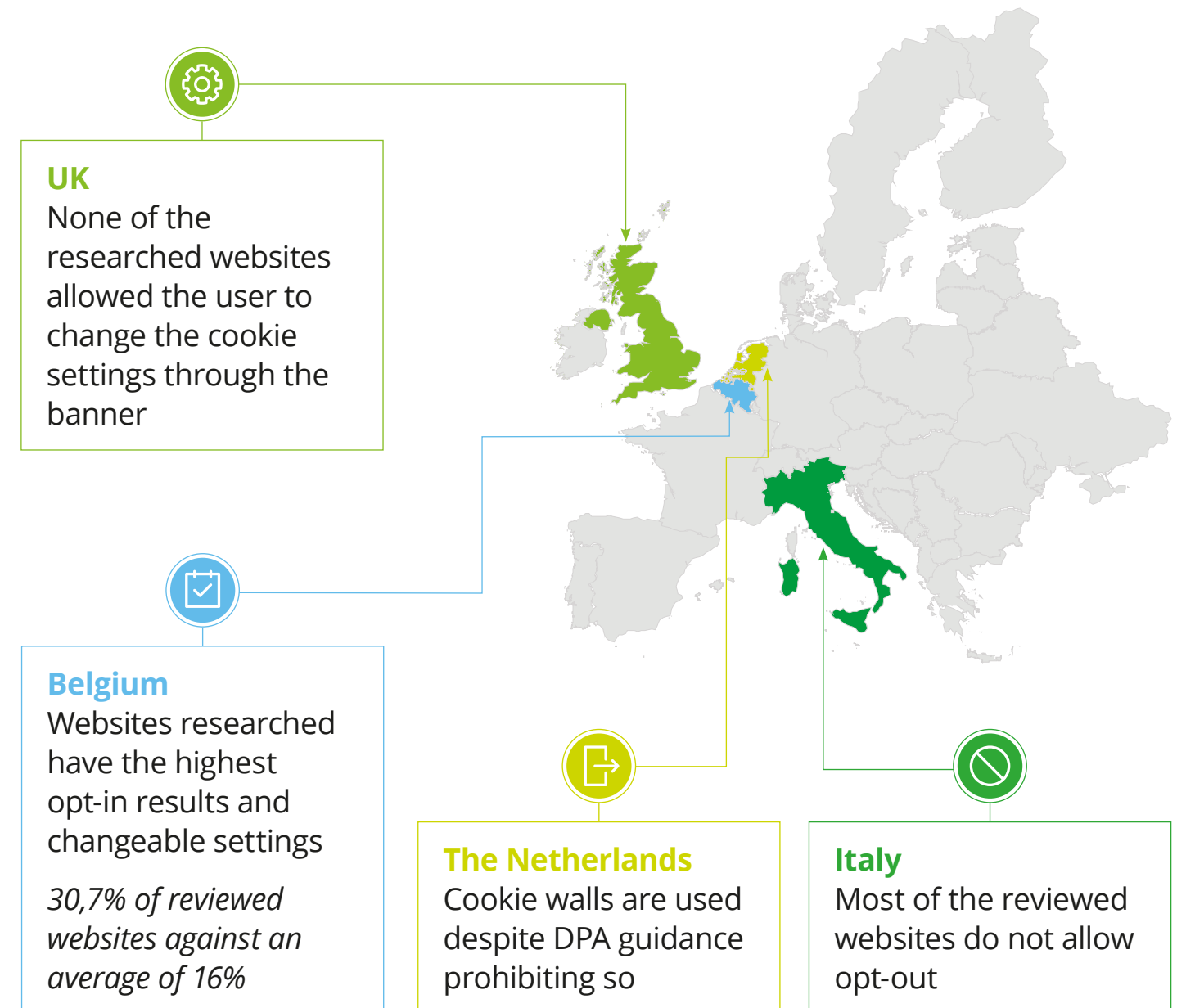
Another interesting fact is to see how the text length of cookie banners varied. In order to be transparent, it is good practice to give all information but in a concise and easily understandable way. In the Netherlands and Greece the average characters used were respectively 388 and 394, where the cookie banners in the UK for instance had an average of 229 characters.

The differences in findings can come from specific local legislation or guidelines. For example, the Irish and Norwegian authorities prescribe that browser settings can be seen as consent, making the necessity of an opt-in less relevant. See [Insights on the actions of authorities for more information.](#)



The ePrivacy Directive was implemented in each country's national legislation. When the ePrivacy Regulation will enter into force, the rules surrounding cookies will be harmonised throughout the Union, which will make these national implementation laws obsolete. This will improve the level playing field for all parties within the Union.

Our dataset includes a selection of websites from Belgium, Denmark, Finland, Greece, Iceland, Ireland, Italy, the Netherlands, Norway, Sweden, Switzerland and the UK



Insights on the actions of authorities

As national discrepancies exist in the implementation of the ePrivacy Directive and the GDPR, national authorities also differ in their regulatory capabilities, the course of actions taken (if any) and the guidance they provide. Some authorities are more active whilst others might wait for the ePrivacy Regulation to be final. We share our insights on the actions taken by some of the national data protection authorities.



Which regulatory body is in charge?

In Italy, Ireland, Switzerland, Norway and the UK, the Data Protection Authority (DPA) is responsible for monitoring compliance with both the GDPR and the implemented ePrivacy Directive.

However, it is not always the data protection authority that is in charge of monitoring compliance with the rules regarding ePrivacy. In some countries like Belgium, Denmark,, Finland, Greece, Iceland, Sweden and the Netherlands, these tasks fall within the mandate of other public bodies, such as the Authority for Consumers & Markets, the Telecom Authority, the Postal Authority or the Business Authority.



Differences between views and guidance of authorities

In view of the growing use of technologies regarding cookies and with the ePrivacy Regulation coming up, a few DPAs have started to publish guidance on cookies.

The Danish Business Authority has written a specific **Cookie Order** as guidance to the information and consent required when placing cookies.

The Irish Data Protection Commission provides more general information such as type of cookies available.

The Dutch and British Data Protection Authority have published general information regarding types of cookies and their use as well as covering specific cookie-related topics. In the Netherlands, the DPA does enforce requirements under the ePrivacy Directive but does not enforce the Telecommunication Act, which also governs cookies. Other countries do not have a specific legislation regarding cookies, such as Iceland. Consequently, no regulatory guidance on the use of cookies has been issued there yet.



Cookie wall guidance in the Netherlands and the UK

The guidance from authorities differs regarding the use of cookie walls. A cookie wall only allows you to access a website after you give your consent for the placement of cookies. The Dutch Data Protection Authority has published **guidance** on the use of cookie walls and states that with a cookie wall, consent is not considered 'freely' given. This, because one cannot refuse to give consent without adverse consequences.

The Dutch Authority **announced** that it will investigate organisations with non-compliant cookie practices. The ICO has taken a more **nuanced approach** saying that in some circumstances, the cookie wall approach is inappropriate: cookie walls are prohibited if they make 'general access' to a website subject to conditions requiring users to accept non-essential cookies. This paves the way to using cookie walls for specific website content, when used for a legitimate purpose.



Varying views on consent through browser settings

Views regarding browser settings also seem to differ as the Irish authority as well as the **Norwegian authority**, accept browser settings as consent. However, other countries do not see the browser settings as given valid consent.

The **ICO says** that at present, 'it is likely not all users will have the most up-to-date browser with the enhanced privacy settings needed for the settings to constitute an indication of consent'.

The references above represent merely a selection of available sources.

Four cookie cases explained

Both supervisory authorities and courts are taking action against non-compliance with cookie requirements. Multiple cases concerning cookies made it to the Court of Justice of the European Union. These cases show that there is a need for more clarification regarding the placement of cookies. If that clarification will come with the ePrivacy Regulation is yet to be seen.



Planet49

The Planet49 case relates to consent and transparency requirements regarding the use of cookies and similar technologies. The case reached the German Federal Court of Justice, referring it to the Court of Justice of the European Union (CJEU) for preliminary ruling. The CJEU delivered its judgment in October 2019.

The case involved an online lottery service, which used two pre-ticked checkboxes in order to seek consent with its users for placing cookies. The CJEU judged that pre-checked boxes are not sufficient in order to obtain valid consent for placing cookies on a user's device, as it does not constitute an unambiguous indication of the wishes of the data subject. This is in line with the requirement that only active behaviour on the part of the data subject is viewed as giving consent.

For a reference to this case, please click [here](#).



Facebook

On 16 February 2018¹, the Chamber of the Court of First Instance of Brussels judged that Facebook's use of cookies infringed on Belgian Privacy laws by not having obtained valid consent and no other legal basis to rely upon. The court demanded Facebook to stop:

- Placing non-functional cookies for tracking purposes
- Collecting and using non-functional cookies for tracking purposes in a disproportionate manner
- Using misleading information regarding the scope of measures that Facebook uses to control the use of cookies

A penalty of EUR 250,000 per day was set on not complying with the ruling. Facebook brought the case to the Court of Appeal of Brussels that brought the case to the Court of Justice of the European Union in order to clarify this issue. The decision of the Court of Justice is still pending.

¹ Court of Appeal of Brussels – 18N-2018/AR/410

For a reference to this case, please click [here](#).



Fashion ID

A German online clothing retailer, Fashion ID, embedded Facebook 'like' buttons on its website. The buttons automatically transmitted personal data to Facebook and Facebook placed cookies on the visitor's device.

In the preliminary ruling of July 2019, CJEU held that FashionID and Facebook are joint controllers, facing equal requirements regarding the personal data which is processed. One of the consequences is that the operator of a website must obtain consent prior to the collection and transmission of data. Visitors must also be provided with information regarding the collection and transmission of their data, prior to this taking place. The requirements to obtain consent and to inform do not have to cover the subsequent processing of personal data by Facebook.

For a reference to this case, please click [here](#).



Jubel.be

The Belgian DPA has fined an online content platform for the violation of cookie requirements of the GDPR. With this first enforcement action around cookie compliance, the DPA wanted to set the example for other Belgian organisations.

Users of the website Jubel.be did not obtain valid consent for the placement of non-strictly necessary cookies. Also, the transparency level of the cookie policy did not meet the mark as set out by the GDPR.

The decision of the DPA led to a fine of EUR 15000.

KnopsPublishing, the owner of Jubel.be, posted a blogpost to inform their readers about the decision.

For a reference to this case, please click [here](#).



Performing a check of your own website: a Do-It-Yourself (DIY) guide



1. Know what to check
 The first step of this checking process is knowing what you want to assess based on your internal cookie and personal data policy. The legal requirements and your organisation's risk appetite will therefore determine this checklist.

- Does the cookie notification comply with transparency requirement?
- Are individuals able to accept or decline cookies?
- Are only strictly necessary cookies placed before obtaining consent?
- Are cookies placed according to given consent?
- Can consent effectively be withdrawn?

2. Start with a clean browser and a clean internet connection
 Any browser can be used to review your website. Be sure to delete all browsing data before visiting your site for a check. This ensures that previously placed cookies do not interfere with your results. With regard to the internet connection, make sure to use a connection that is not filtered by the Internet Service Provider or organisation that provides the connection. This will avoid that items, including cookies and other tracking mechanisms, are filtered out.

3. Visit your website for the first time
 In most browsers you can view the placed cookies by pressing "F12" and finding your browsers cookie tab. Are only strictly necessary cookies placed or also cookies which require consent? Look at how your website gives a cookie notification: are you able to use the site or does the notification block the access to the website? Does the notification explain which cookies will or can be placed? Does the notification nudge users to accept all cookies? The answers to these questions can tell you something about the level of compliance with the information and consent requirements.



4. Changing the settings
 Now its time to check the cookie settings to see if users can easily change their consent. After accepting all cookies can you easily adjust the cookie settings? Are the cookie settings prominently displayed? What kind of cookie options are you offered as a user? This step checks whether the right to withdraw consent is effectively enabled.

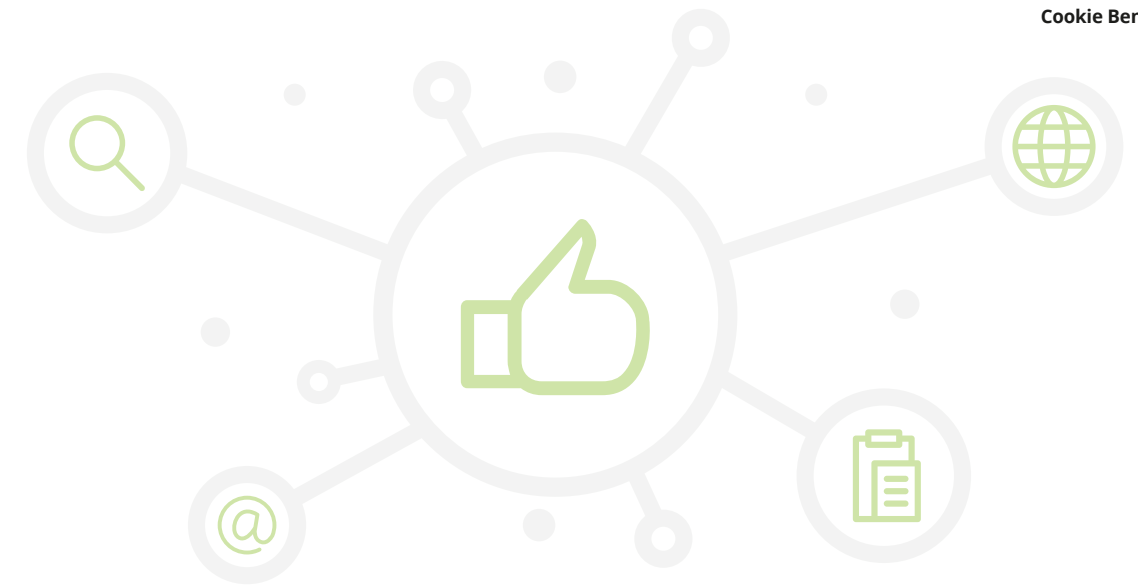
5. Are cookies placed in line with the chosen settings?
 It is important to assess whether the setting changes (step 4) are reflected in the factual placement of cookies. When accepting all cookies: check whether any additional cookies are placed. Once you opted out from all cookies again: have the placed cookie values changed or are any cookies removed? Did all non-strictly necessary cookies disappear?

6. Review your findings
 Based on the information you gathered going through the previous steps you can answer the questions of step 1. Most organisations take a risk-based approach towards compliance, weighing the benefit of compliance against the added value of placing cookies without proper consent. This is reflected in the site functionality before accepting cookies, ease of accessing cookie settings, and strict removal of cookies once users withdraw consent. This DIY guide enables you to gauge how your organisation fits into this compliance spectrum and whether this position is in line with your organisation's risk appetite.



Creating a user-centric cookie experience

Taking advantage of our experience of building digital solutions, our knowledge of cookie regulations and our insights in industry best practices, our team developed a methodology to check cookies practices against relevant compliance requirements. This process is partly automated through a tool which allows the execution of in-depth checks for sites, specifically tailored to fit the unique needs of each organisation.



Tailoring the assessment to your needs

Our methodology enables you to perform checks against a wide set of criteria. This includes controls which are linked to external requirements, such as Security standards, ePrivacy Directive and GDPR. Also internal organisational requirements can be configured as controls.

Cookie discovery and classification

Your organisation can obtain insight into the cookies used on the selected URLs. This includes an insight in the different categories of cookies placed, and whether or not these are placed by third parties.

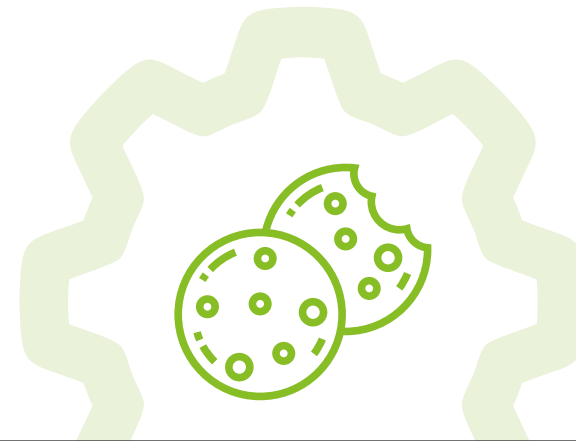
Practical application of consent requirements

The tool makes it possible to automatically check for specific categories of cookies and whether cookies are placed correctly after consent was given.



Covering your organisation's online presence

The automated process facilitates the check of large numbers of URLs. It allows you to check whether internal policies are incorporated into websites. In addition to websites, it is also possible to check compliance for your organisation's social media pages.



How it works

Checking your organisation's online presence against cookie requirements can be done in three steps:

1. Provide a list of URLs to be checked for compliance
2. Select the requirements against which each URL will be checked
3. Results per URL are generated through the automated cookie tool

There are no limits in the amount of the URLs list, the software will check against any number of sites, one by one.

Defining a user-centric cookie experience

Deloitte supports organisations in creating a cookie compliant, yet user-friendly and branded privacy experience for online consumers. Based on your organisation's envisioned functionality and use of cookies, we can explore how to use a more consumer-centric approach as a competitive advantage.



Contacts

This report was written with the help of this team of Deloitte privacy experts.



Annika Sponselee
The Netherlands
Privacy and Cyber Partner
Head of Deloitte Data
Privacy Services
asponselee@deloitte.nl
+31 6 1099 9302



Peter Gooch
United Kingdom
Privacy and Cyber Partner
pgooch@deloitte.co.uk



Nicole Vreeman
The Netherlands
Senior Privacy Manager
nvreeman@deloitte.nl
+31 6 2072 8618



Erik Luysterborg
Belgium
Privacy and Cyber Partner
EMEA Privacy & Data
Protection Leader
eluysterborg@deloitte.com



Emma Haenebalcke
The Netherlands
Senior Privacy Consultant
ehaenebalcke@deloitte.nl
+31 6 5007 0213



Tommaso Stranieri
Italy
Privacy and Cyber Partner
tstranieri@deloitte.it



Zhasmina Kostadinova
The Netherlands
Senior Privacy Consultant
zkostadinova@deloitte.nl
+31 6 2252 1561



Line Vedel Perlman
Denmark
Privacy and Cyber Partner
lperlman@deloitte.dk



Annex – Research methodology

The following research questions were used to check the level of compliance with cookie requirements of the websites in scope:

- 0. Information**
 - Website URL
 - Date
- 1. Cookie service providers**
 - Does the website have a cookie notification?
 - State whether it is a banner, pop-up or wall?
 - Which cookie banner/ Consent management platform is used?
- 2. Cookie banner transparency**
 - Copy-paste the cookie banner
 - Does the cookie banner contain a link to the cookie policy?
 - Do the colours and fonts in the cookie banner relate to the choices given?
- 3. Cookie consent**
 - Does the user have to opt-in or opt-out of cookies?
 - What are the options given to the user in the cookie-banner?
 - Is it possible to adjust the cookie settings directly from the cookie banner?
 - When you accept all cookies, how many cookies are placed?
- 4. Third party cookies**
 - What types of 3rd party cookies are placed?
 - Which 3rd parties place the cookies?
 - How many 3rd party cookies are placed?
- 5. Security**
 - Which security headers are in place?
 - Does the website use HTTPS?
- 6. User-experience (all questions use dropdown yes/no/unsure or N/A)**
 - Are there any images, graphs or videos used to facilitate the message conveyed by the cookie banner? Is the brand of the organisation / website mentioned in the cookie banner?
 - Are the colours of the cookie banner similar to the colours of the website?
 - Are the buttons used in the cookie banner clear and accessible?
- 7. Remarkable findings**
 - Does the website have a public user-admin interface?
 - Does the cookie banner load together with the website?
 - Did you notice any dead links? Explain which links and where:
 - Did you notice anything else? Explain what:
- 8. Industry & country**
 - 8.1. What is the industry of the website?
 - 8.2 What is the country of the website?

We used Vivaldi browser to manually extract both the relevant website information and the raw cookie data. For every website, we logged which cookies were placed, after deleting browser history. This to ensure that previously placed cookies do not interfere with our results. We counted and categorised the cookies placed per type of cookie (strictly necessary, functionality, performance, advertisement) and per party (first party and third party cookies). We based the classification on our professional knowledge of cookies, combined with the information on cookies which is made publicly available by cookie suites. Cookies that could not be identified, were excluded from detailed analyses on the different cookie types and parties placing the cookies.

Overview of the websites reviewed

Below is the overview of the amount of websites reviewed per country. The choice was made for two websites per country for each industry. Amounts differ based on the availability of websites within each country. Websites were chosen based on the following requirements:

- Accessibility in the respective country. This means that the language of the website is often used in the country, or the website uses the country specific domain (e.g. in the Netherlands this is .nl).
- The organisation and its website are fully operational.
- The organisation is a provider of goods and services, which has a large consumer base within the respective country in its industry.
- The quality of the provided goods and services are perceived to meet high standards.
- Optional: Headquarters of the organisation are established in the respective country.

Besides country-specific websites, we also looked at a number of websites with a cross-European reach. These websites fulfil the above criteria, with the addition that their consumer bases reaches over the countries in scope.

	Technology, media & telecom	Consumers	Energy, Resources & Industrials	Financial Services	Life Sciences & Health Care	Government & Public Services
Belgium	2	2	2	2	2	2
Italy	2	2	3	4	2	2
Greece	2	2	2	2	2	2
Ireland	2	2	2	2	2	2
The Netherlands	2	2	2	2	2	1
Denmark	2	2	2	3	2	2
Finland	2	2	2	2	-	2
Iceland	2	2	2	2	2	2
Norway	2	2	2	2	2	2
Sweden	2	2	2	2	2	2
Switzerland	2	2	2	2	2	2
UK	2	9	2	2	4	4
Websites with a cross European reach	-	4	3	2	1	-
Total	24	35	28	29	25	25

Notes



Deloitte.

Deloitte Risk Advisory B.V. is part of a Dutch group of firms providing professional services, including audit, consulting, finance, risk management, tax and related services to clients. This Dutch group of firms, all active under the brand 'Deloitte', is part of the international network Deloitte Touche Tohmatsu Limited ('DTTL'). DTTL is a UK 'private company limited by guarantee'. Deloitte NSE LLP is a member firm of DTTL. The local Dutch Deloitte entities, including Deloitte, are affiliates of Deloitte NSE LLP. The member firms of DTTL, including the affiliates of these member firms, are all separate and independent legal entities which cannot obligate each other, nor DTTL.

© 2020 Deloitte Risk Advisory LLC. All rights reserved.

Designed by CoRe Creative Services. RITM0347555