

ICTRECHT

FACTSHEET

Cookies: privacy by design and default

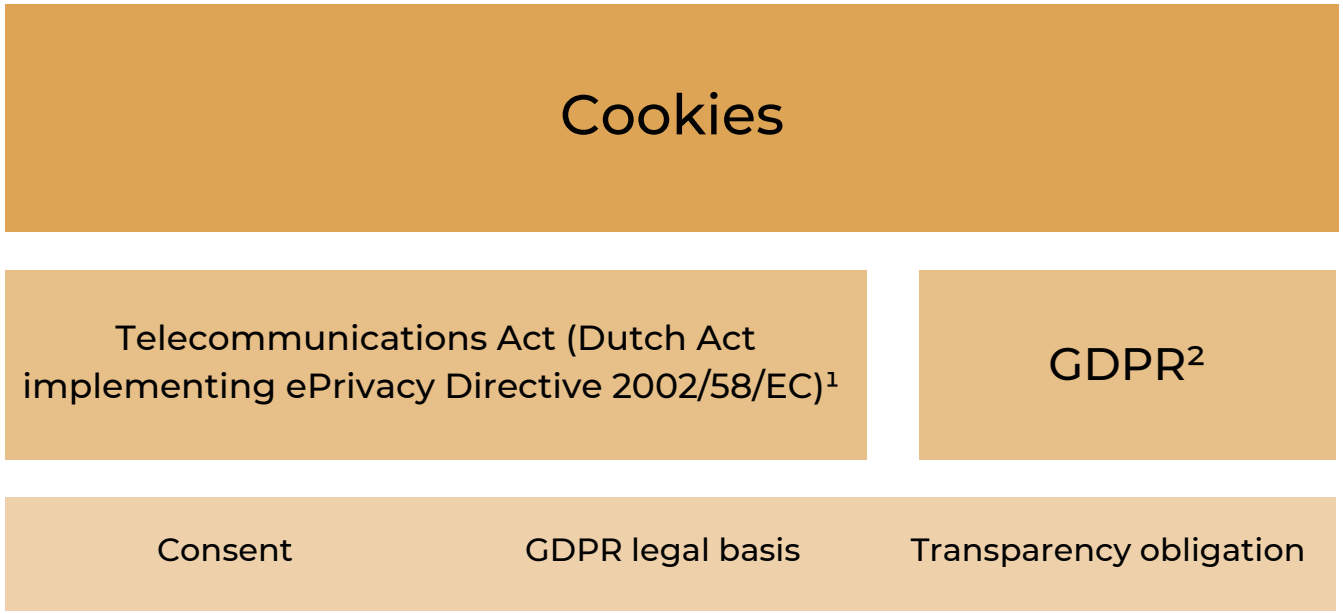
Introduction

In this factsheet, we describe what cookies are and the rules established by law regarding them. As tracking cookies are the most heavily regulated, this factsheet focuses on tracking cookies.

This factsheet is titled "Cookies: privacy by design and default." By this, we mean that the technology is designed and configured in such a way that it enforces compliance with applicable privacy legislation. Only in this way is it ensured that cookie practices align with the prevailing legal frameworks.

This factsheet covers the following topics:

- We distinguish between the different categories of cookies and how they work.
- We describe the relationship between cookies and personal data.
- We outline the legal framework regarding cookies.
- We answer key questions about cookies.



[1] English translation of Dutch law

[2] GDPR: General Data Protection Regulation



1. Cookies: small files, big intelligence

Cookies are small files that a website owner places on a visitor's device. For example, on a computer, laptop, smartphone, or tablet. This allows the website owner to track the website visitor and collect or store information about the website visit or about the visitor (or their device).

These cookies and other similar technologies can facilitate unlawful conduct towards data subjects by infringing upon their privacy rights. Because fundamental rights are involved, strict rules apply under the Telecommunications Act (Tw, unofficial English translation of Dutch law) and the General Data Protection Regulation (GDPR) to technologies that track website visitors and collect data.



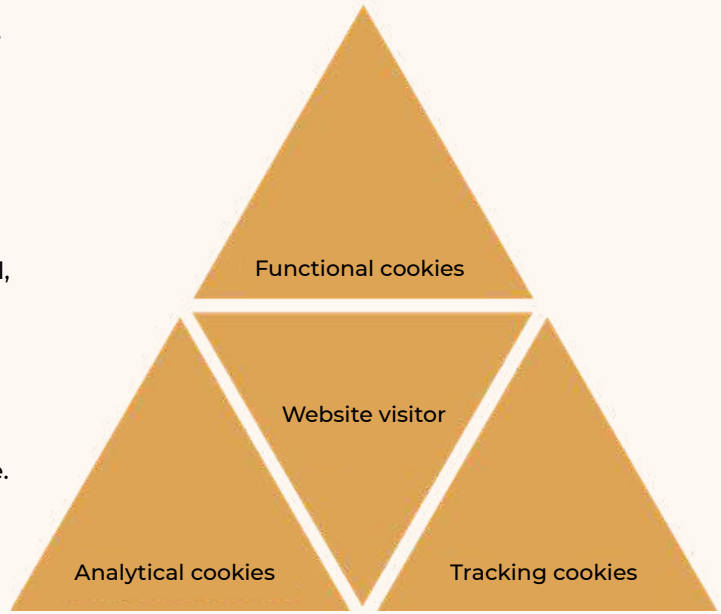
Three main categories of cookies are distinguished:

1. Functional cookies
2. Analytical cookies
3. Tracking cookies

1.1 Functional, analytical and tracking cookies

Cookies are used to identify and track users. Various technologies for identifying and tracking users are creating grey areas. Consequently, it is becoming increasingly difficult to determine the type of cookie placed on visitor's device and whether the cookies in question are functional, analytical, or tracking.

Below, we describe the main characteristics of the three categories of cookies, their purpose, and the applicable consent regime.



Functional cookies	Analytical cookies	Tracking cookies
(no or minor privacy infringement)	(minor privacy infringement)	(major privacy infringement)

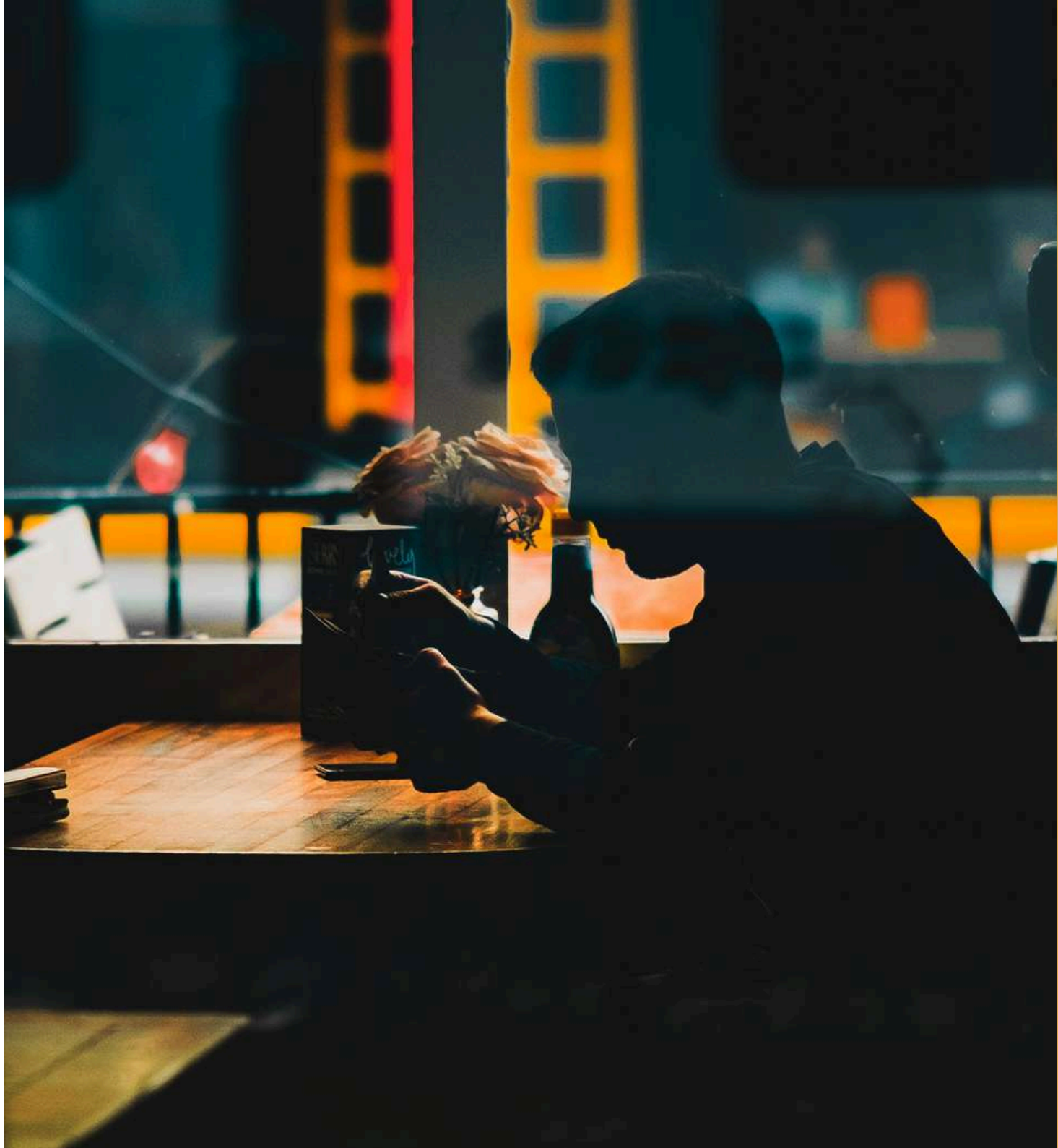


Type of cookie	Description	Purpose	Consent
Functional cookies Article 11.7a(3)(a) of the Dutch Telecommunications Act Article 6(1)(f) of GDPR	Cookies used to ensure a website or app functions properly, and which are therefore technically necessary to guarantee the quality and effectiveness of the website's operation. Upon visiting a website, the visitor's IP address is processed and functional cookies are placed on the visitor's device by the website owner. These cookies have little or no impact on the website visitor's privacy.	These cookies enable the execution of communication or are strictly necessary to ensure that the provider of an information society service requested by the user is able to deliver that service. This involves, for example, saving a password to allow a visitor easier access to a specific website, or remembering default settings.	These functional cookies may be placed and/or read without consent. If consent is not required under the Dutch Telecommunications Act (Tw) for placing or reading a cookie, no separate consent is needed under the GDPR for any subsequent processing of personal data derived from that cookie. This processing activity can rely on legitimate interest (Article 6(1)(f) GDPR) as the lawful basis of processing for the party (or a third party) responsible for this processing activity.
Analytical cookies Art. 11.7a(3)(b) Dutch Telecommunications Act (Tw) Art. 6(1)(f) GDPR	Analytical cookies are intended to improve the use of the website/app and their services. These cookies collect information about visitor numbers, clicks on links and videos, and on which devices the website or app is visited. Visiting a website involves the processing off personal data when the visitor's IP address is recorded and analytical cookies placed. An IP address will always be processed when visiting a website, because a web server relies on it to deliver the requested information to the right location.	The processing serves the sole purpose of generating aggregated insights for the website administrator about their own website, which are necessary to maintain and improve it. The website administrator must limit the impact on a visitor's privacy and ensure that no less intrusive alternatives exist to achieve the same purpose.	An IP address allows for the identification of a device, such as a computer, and thereby enables the identification of a natural person. The requirement to obtain consent does not apply insofar as analytical cookies are configured in a privacy-friendly manner. The party responsible for the processing (or a third party) may rely on 'legitimate interests' as the legal basis for this processing, provided they carry it out in a privacy-friendly manner.
Tracking cookies Art. 11.7a(1) Dutch Telecommunications Act (Tw) Art. 6(1)(a) GDPR	A cookie can be classified as a tracking cookie if its purpose is to map (individual) visitors and their browsing behaviour, and through which personal data is therefore processed. Tracking cookies typically store a unique, randomly generated ID assigned to a website visitor's browser via tracking cookies. The cookie provider reads the same tracking cookie every time the visitor uses that browser to visit a linked website.	A party other than the website (domain) chosen by the user often places and reads these cookies to collect data on the user's browsing behaviour, which, can subsequently be used for marketing purposes. The primary aim is to collect and analyse internet user's browsing behaviour, interests, and other relevant data for commercial purposes.	Article 11.7a(1) of the Dutch Telecommunications Act (Tw) and the GDPR require prior consent from the data subject for the use of tracking cookies.

1.2 First party cookies and third-party cookies

A first-party cookie is connected to the same web server as the website visited. This means the website itself places cookies on visitors' devices, for instance, to tell different browsers apart and how to understand the website is used and which pages are visited most frequently.

Third-party cookies, on the other hand, are placed and read by ad servers that belong to third-party cookie providers, doing so in response to a so-called cookie call.



2. Cookie services

Website and mobile application owners actively seek insight into how visitors use their platforms and other online environments. The AdTech industry: encompassing digital marketing, media advertising, and real-time auctions, capitalises on this demand by offering services such as advertising and analytics tools that use technologies like cookies to track internet users. When operators install such a service, it places cookies on computers and/or mobile devices, sometimes through a third-party website.

Over the years, a complex, hard-to-understand, and non-transparent ecosystem consisting of many different parties has grown around cookies. These actors include websites and app owners, operators, providers or advertising and analytics services, advertising platforms, publishers, and advertisers. Each actor exercises influence, control and/or decision-making authority over the development and use of cookies and therefore shares responsibility for it. Courts have established that actors cannot hide behind one another, for example, by claiming they outsourced certain tasks to a third party or that another party designed the technology or configured the settings.

Analytical service	Focused on analysing the behaviour of website visitors.
Advertising service	Websites that offer advertising space to advertisers by making use of an advertising service. Through an advertising service, advertisers can display their ads in the advertising space on their own websites as well as on websites managed by third parties.



2.1 Tracking cookies in action: from cookie decision to data use

Six phases describe the process surrounding the use of cookies, as outlined in the figure below. Organisations must apply privacy by design and by default starting even before they select a service, continuing through how they use cookie information. They must safeguard privacy during the selection and design process and when configuring a service.

1. Choosing	2. Integrating	3. Cookie Call	4. Placing	5. Reading	6. Using
Select advertising and analytics services	Integrate a snippet of cookie code into the website	Cookies are called upon when visiting the website	Placing cookies on the website visitor's device	Upon (new) visit, a new call ensures the cookie is read by the Ad Server.	After the cookie is read, it is decided whether cookie(information) is used

Six phases of cookie-processing

1. **Choosing:** the website owner chooses a specific cookie service, known as an ad server.
2. **Integrating:** the website administrator integrates a snippet of code, such as JavaScript, into the website.
3. **Cookie Call:** when the website is visited by a visitor, the cookies are called upon.
4. **Placing:** cookies are placed on the visitor's devices (laptop, smartphone, tablet, and other devices used).
5. **Reading:** once a (new) website visit occurs which makes use of the same code, the cookie is read by the ad server.
6. **Using:** deciding whether the cookie information will be used.

How cookies work: calling, invoking and placing

1. **Loading the website:** when a website loads, the visitor's browser sends an HTTP request to the website's web server.
2. **Cookie call:** once the website has loaded, the code automatically sends a request to the ad server linked to the cookie (a "cookie call").
3. **Invoking cookies:** the content of the cookie code determines which cookies will be invoked during the cookie call.
4. **Placing cookies:** the ad server automatically responds to the cookie call by placing the requested cookie(s) on the visitor's device (set-cookie).

Reading cookies

When the visitor returns to the website, or visits another website using the same cookie code, a new cookie call ensures the ad server also reads the cookie.

Using cookie information

When the cookie is read, the third-party cookie provider decides whether the cookie (or the information contained therein) is actually used for its intended purpose, such as analytics or displaying personalised advertisements.

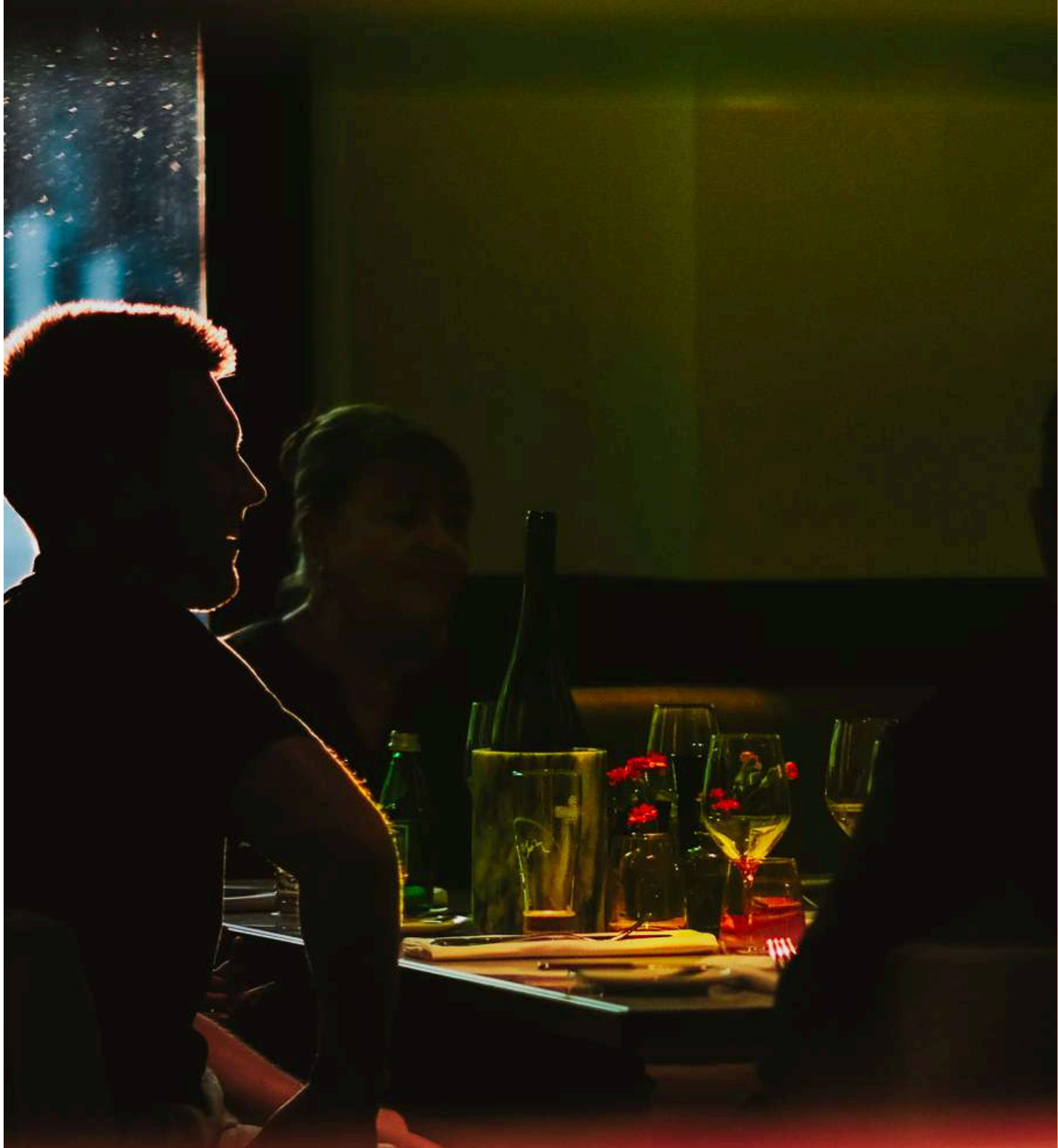
When does processing occur?

Reading personal data for advertising purposes is not the only processing activity that takes place; storing personal data also constitutes processing. Placing tracking cookies, which are automatically filled with personal data once the visitor accesses the website, and subsequently reading that data read, is also a processing activity.

2.2 Creation of user profiles

Tracking cookies are typically used for ‘targeted advertising’: the tailoring of advertisements to individual users. Cookies are placed to capture personal data, enabling the creation of profiles that can subsequently be accessed for advertising purposes.

These user profiles are maintained to recognise users when they visit the internet. Within a fraction of a second, the Real-Time Bidding (RTB) system recognises an internet user and displays an advertisement tailored to them.



3. Cookie regulations

Recital 1 of the GDPR states that the protection of natural persons with regard to the processing of personal data is a fundamental right. Pursuant to Article 8(1) of the Charter of Fundamental Rights of the European Union and Article 16(1) of the Treaty on the Functioning of the European Union, everyone has the right to the protection of their personal data. Individuals may take action against an (alleged) infringement of their fundamental rights.

Therefore, the use of tracking cookies or other similar technologies is heavily regulated. Specifically, for cookies that require consent to be placed and/or read or used on the devices of data subjects, prior valid consent must have been obtained. In other words: placing, reading and using tracking cookies on computers or other devices without prior consent is not permitted. The rules regarding cookies are laid down in the distinguishable processes: placing cookies, reading cookies and using cookie information.

Applicable legal provisions

Dutch Telecommunications Act (Tw):

- Art. 11.7a Tw (cookie provision)

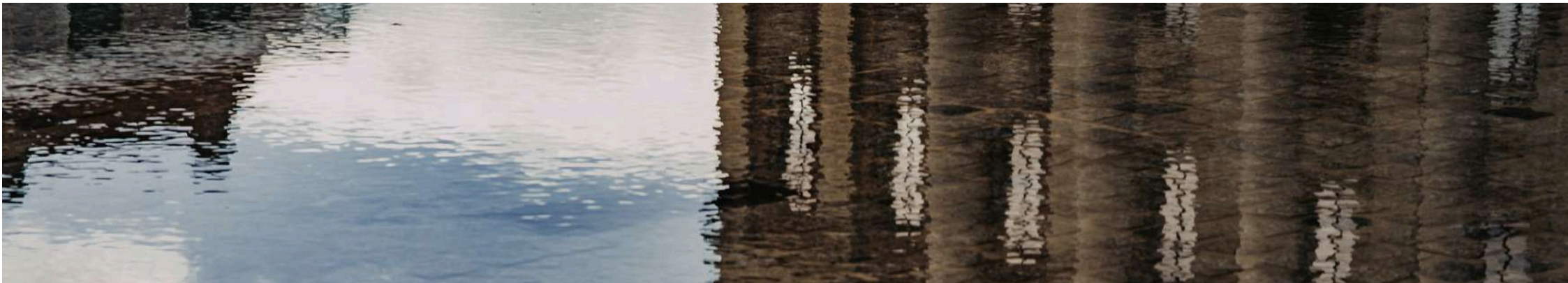
General Data Protection Regulation (GDPR):

- Art. 5.1.a GDPR (transparency)
- Art. 6 GDPR (lawfulness of the processing)
- Art. 7 GDPR (conditions for consent)
- Art. 13 GDPR (information obligation)
- Art. 14 GDPR (information obligation)

Directly or indirectly placing cookies

Reading cookies

Using cookie information



3.1 The “Cookie Law” is a myth. The Dutch Telecommunications Act and the GDPR do exist

Under Article 11.7a of the Dutch Telecommunications Act, you need the user’s prior consent to place and read cookies. The GDPR requires the same for the subsequent collection and processing of personal data.

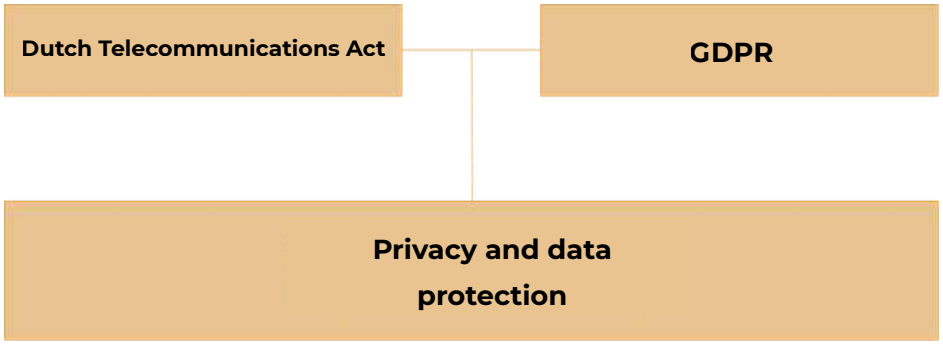
Protection against interference with private life

Article 11.7a paragraph 1 of the Dutch Telecommunications Act implements Article 5 paragraph 3 of the ePrivacy Directive (2002/58/EC). The ePrivacy Directive aims to protect the user against interference with their private life, regardless if that interference relates to personal data. This means that the protection extends to all information stored on a user’s device (also known as “terminal equipment”), not just personal data. The goal is to shield users from hidden identifiers and software entering their devices without their knowledge. In short: placing and reading tracking cookies requires prior consent under Article 11.7a paragraph 1 of the Dutch Telecommunications Act. Where personal data is processed in the course of placing and reading such cookies, the consent requirement of the GDPR applies as well.

Who does the cookie provision apply to?

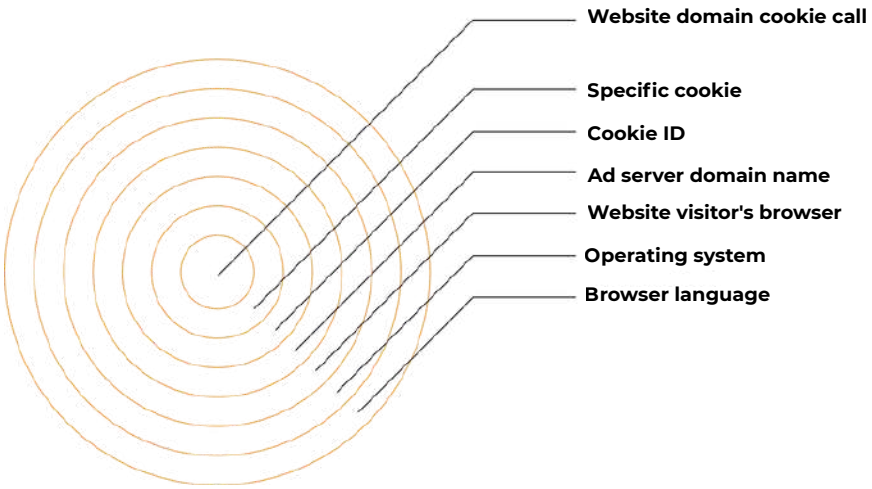
The provision in Article 11.7a paragraph 1 of the Dutch Telecommunications Act is aimed at whoever stores information on a user’s device or to the party that gains access to information already on the device. In other words, the party placing the cookie is the one this provision addresses. This party is often the provider of the relevant website but does not have to be. It can also be a third party that has an agreement with the provider of the website (or an intermediary) allowing it to place or read cookies through the site.

Controllers under the GDPR must have a valid legal basis to process personal data through cookies (Articles 5 and 6 GDPR). For tracking cookies by means of which personal data is processed, this will usually be Article 6(1) (a) GDPR: 'the data subject has given consent to the processing of his or her personal data for one or more specific purposes'.



3.2 What data is processed during a cookie call?

Personal data is recorded by placing tracking cookies that enable the creation of profiles for advertising purposes. Consequently, tracking cookies involve the processing of personal data, such as the user's IP address. However, a cookie also involves the processing of additional (personal) data. When a cookie is called, the visitor's browser sends (among other things) the following data:



Consent and cookie banner

Tracking cookies may only be placed on a user’s computer or device after that user has given valid consent. This requirement stems from the GDPR and the Dutch Telecommunications Act. These two laws differ regarding the consent requirement:

- Article 6(1)(a) GDPR refers to the consent of the data subject (the natural person to whom the personal data relates).
- Article 11.7a of the Dutch Telecommunications Act refers to the consent from the user (a natural person or legal entity using a publicly available electronic communications service).

A cookie banner used to obtain consent must meet all applicable requirements. The use of "dark patterns" when seeking consent through banners is not permitted. Consent must always be based on a free and informed choice, and users must have an immediate option to refuse or adjust their choices.

The following practices are prohibited with regard to consent and a cookie banner:

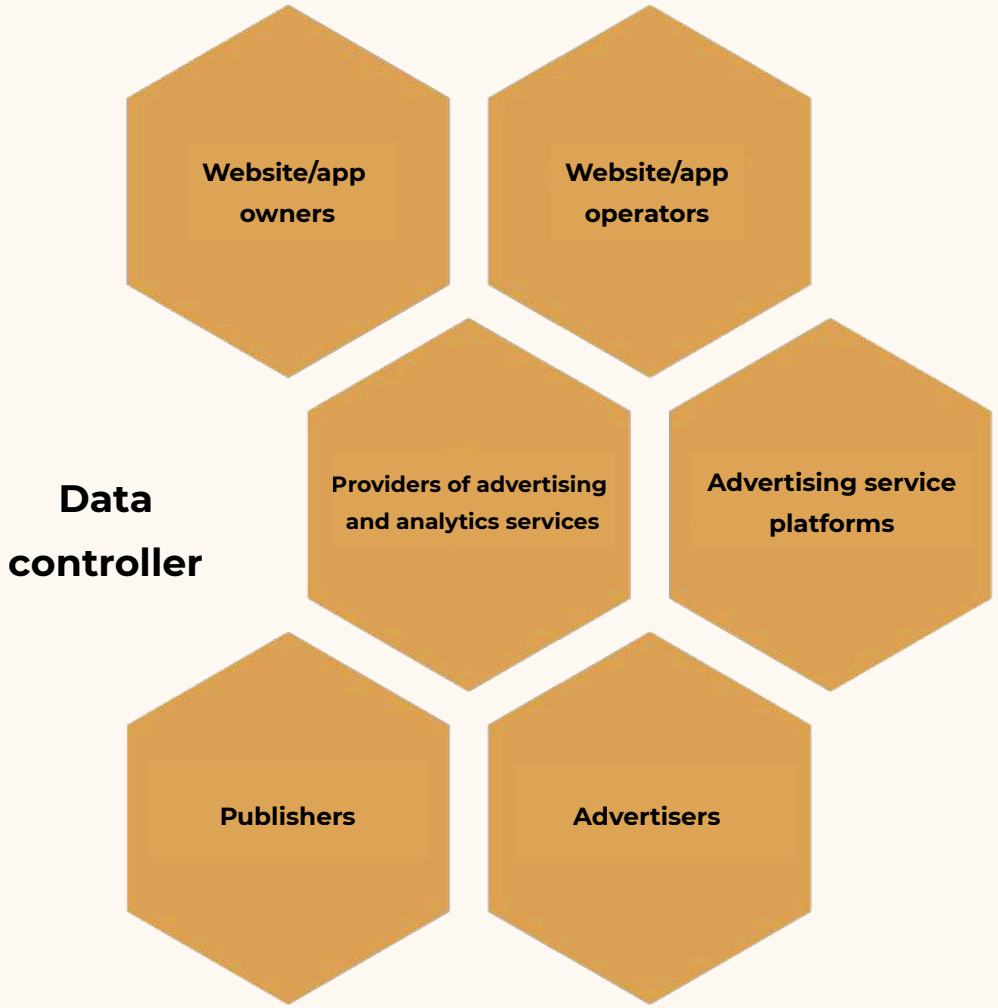
- Placing or reading cookies before the user has made a choice, or after the user has refused consent.
- Designing a cookie banner that makes refusing cookies more difficult than accepting them.
- Using pre-ticked boxes for consent, with only a link to a page containing further information.
- Placing or reading cookies before the website visitor has actively interacted with the cookie banner.
- Ignoring a user’s refusal of cookies.
- Obtaining consent that is not ‘informed’ or not ‘freely given’.

4. Who is the controller?

Who qualifies as a controller when it comes to cookies, and who qualifies as a processor? First, suppliers or service providers that exclusively place cookies on behalf of and for the benefit of another party (the controller) can be designated as processors. In such cases, a data processing agreement is required. However, if a supplier or service provider also places its own tracking cookies or determines the purposes and means of processing itself, it may also qualify as a controller.

In practise, the situation is more complex. Any (legal) entity within the ecosystem that influences the processing of personal data may qualify as a controller. This is the case when they participate in determining the purpose and means of the processing. But who are these parties? Primarily, they are website owners and operators, though all other actors in the ecosystem may also qualify as controllers.

Parties that have developed tracking cookies and make these available to website owners and operators, and with whom agreements have been concluded regarding privacy, may also qualify as data controllers. These various actors in the ecosystem can, as chain partners, also qualify as joint controllers within the meaning of Article 26 GDPR.



5. Cookie statement: duty to inform

A cookie statement serves to inform the data subject and promote transparency about data processing. The controller must actively and proactively inform the data subject about how their data is processed. This enables data subjects to monitor what happens to their data and, where necessary, to challenge certain processing activities or unlawful conduct by the controller. After all, the data subject can only exercise their statutory rights if they are aware of the processing taking place. The controller bears the burden of proving that the processing is lawful, which includes ensuring that the data subjects are adequately informed about the data processing beforehand.



It is therefore up to the controller to demonstrate that it has met its duty to inform and that the processing of personal data is lawful, fair, and transparent. Any processing about which the controller has not properly informed the data subject is unlawful. In the context of cookies, Article 11.7a, paragraph 1, of the Dutch Telecommunications Act provides that storing information on, or gaining access to information from a user's device is only permitted if:

- the user is clearly and **fully informed** (at minimum, about the purposes for which the information collected through cookies is used), and
- the user has given **consent**.

The duty to inform must be fulfilled in accordance with both the Telecommunications Act and the GDPR. The relevant legal provisions regarding the duty to inform are set out below.

Legal provision	Information obligation
Article 11.7a, paragraph 1 Dutch Telecommunications Act	Informed consent.
Article 5(1) under (a) and (2) GDPR	The controller is responsible for compliance with the transparency obligation and must be able to demonstrate such compliance. Personal data of the data subject must be processed in a manner that is lawful, fair, and transparent.
Article 12 GDPR	In accordance with Articles 13 and 14, appropriate measures shall be taken to provide the data subject with information relating to the processing in a concise, transparent, intelligible and easily accessible form, using clear and plain language.
Article 13 GDPR	When personal data are collected from the data subject, the controller informs the data subject about the collection at the time of the collection in accordance with Article 13 GDPR.
Article 14 GDPR	When personal data have not been obtained from the data subject directly, the controller shall provide the data subject with the information referred to in Article 14 GDPR.

FAQ: Frequently Asked Questions

When using cookies, we advise complying with the legal requirements in place and apply the principes of privacy by design and by default. In practise, the reality of using cookies is complex and challenging. Various situations may arise when placing and using cookies. For that reason, we answered a number of essential questions below.

Question

Is it sufficient if I disclose our identity and processing purposes in our the cookie statement?

Answer

No, it is not sufficient to only disclose your identity and processing purposes. Often, you will need to provide further information to the data subject, insofar necessary to ensure fair and lawful processing. For complex, technical or unexpected data processing, such as cookies, controllers must explain the main consequences of the processing separately and in unambiguous language, in addition to providing the information required by Articles 13 and 14 GDPR.

The controller must always consider if the circumstances suggest that the data subject has a genuine interest in receiving further information, and if so, what the scope of that information should be.

Question

What steps are needed to use analytics tools like Google Analytics in a privacy-friendly way?

Answer

For analytical cookies, you can take precautionary measures to minimise unwanted consequences for website visitors. These measures include:

- Applying privacy-friendly settings. For example, according to the Dutch Data Protection Authority's Guide for Google Analytics, by:
    - following steps 1 to 4 from the guide;
    - configuring Google Analytics in a privacy-friendly manner according to the step-by-step plan.
- Concluding a data processing agreement with the service provider ((sub)processor), which includes, among other things, that the last octet of the IP address is masked.
- Ensuring that no user IDs are linked to IP addresses.
- Ensuring that (sub)processors are not permitted to use the (masked) IP addresses for their own services.
- Guaranteeing that (sub)processors are not permitted to use the (masked) IP addresses for their own services. Informing users in the privacy/cookie statement that such a cookie service is being used and that steps 1 to 4 from the Dutch DPA's Guide have been applied.
- Informing visitors upon their first visit about the use of functional and analytical cookies.

Question

If we only place cookies without reading them, are we processing personal data?

Answer

Processing of personal data does not only occur when cookies are read for advertising purposes. Storing data in a cookie is already sufficient. Processing also includes placing tracking cookies, which are then automatically 'filled' with personal data as soon as someone visits the relevant website, with the purpose of reading this data later.

Question

Does the fact that we do not process any name and/or address via a cookie mean that we are not processing any personal data?

Answer

The concept of ‘personal data’ is interpreted broadly and is not limited to name, address, and place of residence of a data subject. It is sufficient if data relating to identifiable data subjects can be linked to an ‘identifier’ and recorded for further processing, for example, for advertising purposes.

Question

Does processing a cookie ID count as processing personal data?

Answer

This is an incorrect assumption. Apparently, there is a belief that a cookie ID alone would be insufficient to directly identify a natural person. However, according to the GDPR and established case law, a cookie ID is considered personal data. A cookie ID is an online identifier that is also transmitted along with the internet user's IP address. This links data of individualised data subjects to an 'identifier' and records it for further processing.

Question

Am I allowed to contractually outsource the collection of consent for cookies to my partners?

Answer

Yes, that is allowed, but you remain responsible for ensuring that consent is obtained in a legally valid manner. If your service provider and/or partner provides information about the placement of cookies and obtains consent, you are not required to do so as well.

However, as a controller you remain personally responsible for ensuring valid and lawful consent for the placing and reading of tracking cookies. This also applies when the supplier/service provider qualifies as a controller. Under Article 26(3) GDPR, you can be held accountable as a controller, regardless of what has been agreed upon contractually with your partners.

Question

We merely provide tracking cookies, surely website administrators are responsible for obtaining consent for the placing or reading of cookies?

Answer

Case law established that providers of tracking cookies cannot hide behind their clients (i.e. website owners and administrators). The obligations under the Dutch Telecommunications Act are not exclusively placed on website owners. Rather, the legislator decided that the obligation set forth in Article 11.7a of the Dutch Telecommunications Act applies directly to **the party that stores information on a user's terminal equipment**, as well as to **the party accessing information stored on that terminal equipment.**

Question

Who in the cookie ecosystem is responsible for obtaining consent?

Answer

In the chain, obtaining consent is usually left to the partners, as they operate the websites that internet users visit. However, all chain partners and their website partners are to be regarded as joint controllers within the meaning of Article 26 GDPR, and data subjects are free to exercise their rights under the GDPR against each individual chain partner.

Question

Do contractual arrangements between supply chain partners have any bearing on the rights of data subjects?

Answer

Data subjects are not bound by the contractual agreements and procedural measures established by the parties within the ecosystem. When it comes to the data subject, all actors involved share responsibility to ensure that personal data are not processed unlawfully, for example without valid consent.

Question

I am a software provider. I do not have any control or responsibility for the use of cookies, right?

Answer

It is a misconception that control rests solely with the website operator. Software providers that facilitate the placing of tracking cookies or places them via the website operator, also exercise a degree of control.

When cookies are placed as part of the services provided by a software provider pursuant to agreements concluded with website administrators, the software provider does indeed exercise control over the use of the cookies and is therefore subject to the obligations regarding cookies.

Question

Is it acceptable to verify whether valid consent has been obtained for the use of cookie information only after a tracking cookie has already been placed and/or read?

Answer

No, this is not in line with the Dutch Telecommunications Act and the GDPR, both of which require that consent must be obtained prior to placing the cookie. Furthermore, this approach enables the systematic breach of these rules, given that cookie information is collected on a continuous basis.

Question

As a supply chain actor, am I required to block the placement of new tracking cookies?

Answer

No, that is not required. Even if an operator has the ability to block the placement of new tracking cookies, there is no legal obligation to do so. This is because the EU legislator deliberately chose an opt-in system, rather than an opt-out system.

Question

How can software providers comply with cookie legislation?

Answer

As a software provider, you can make tools available to partners that make it impossible to place tracking cookies without consent and ensure that this actually leads to a corresponding practice (privacy by design and default).

