Cookies and other data stored on users' terminal devices and the use of such data – Guidelines for service providers

Table of Contents

1 Background and purpose

The Finnish Transport and Communications Agency (Traficom) is responsible for monitoring the confidentiality of electronic communications. The confidentiality of electronic communications also covers the storing of cookies and other data on the use of online services on user devices, as well as the use of this data. The purpose of this guidance is to promote the implementation of confidentiality and best practices concerning the storage and use of cookies and other data describing the use of services or users' actions in online services.

The guidance is intended for everyone who use cookies or similar technologies when implementing and providing websites or other services based on electronic communications, such as mobile applications.

The purpose of these instructions is not to obligate the use of specific technologies, but to instruct service providers to operate as required by law with regard to the storage and use of cookies and other data on user actions in online services, requesting cookie consent and informing users about the use of cookies. Neither are these instructions or the examples herein intended to be exhaustive, and they will be updated accordingly as related technologies and legal practices evolve. This guidebook is not legally binding as such. However, it defines the view of the supervisory authority on lawful and acceptable cookie policies. By deviating from them, service providers assume the risk of potentially unlawful action.

These guidelines have been authored on the basis of two decisions delivered by the Helsinki Administrative Court on 8 April 2021 (H1515/2021 and H1516/2021 / register numbers 20801/2020 and 20848/2020), where the Administrative Court concluded that no valid consent for use of non-essential cookies could be granted through internet browser settings alone. Moreover, the Administrative Court considered the Finnish Transport and Communications Agency Traficom the competent authority on matters related to cookie regulation and supervision of the use of cookies. According to the Administrative Court, Traficom is also in charge of matters related to the interpretation of consent in questions relating to the use of cookies.

These guidelines have been compiled in collaboration with the Office of the Data Protection Ombudsman, the competent authority in matters related to the processing of personal data.

2 Scope of application

These guidelines have been created for service providers who use cookies and similar technologies to store or access information stored on user devices in the provision of websites and electronic communication services.

Service providers should, at minimum, consider the following matters when using cookies or similar technologies as part of the implementation of services based on electronic communications that they offer:

1. What cookies or similar technologies will the website or the service use or intend to use?
2. How can the cookies be classified into essential and non-essential cookies from the perspective of the service in question?
3. How is information concerning the cookies and their purpose of use offered to the users of the services in a form that is clear and understandable to them?
4. How is consent for non-essential cookies requested from users and how are the users offered the option to modify cookie settings afterwards or to withdraw their consent?

These matters are discussed in sections 2 to 5 of the present guidelines. First, we will discuss what is meant by cookies and other similar technologies.

Cookies are small text files stored on user devices while using websites. Cookies contain data generated during website use, and also store data between sessions. Cookies and similar technologies enable the typical functionalities of modern websites, such as logging in and maintaining the login session for the duration of navigating on the site, or the shopping cart functionalities of online stores. Without the use of cookies, websites or services would be unable to remember anything about the users and their choices and inputs.

While these guidelines primarily refer to cookies, it should be kept in mind that there are other technologies with functionalities similar to cookies. These technologies are subject to the same rules, and, as applicable, to the instructions given in these guidelines. The term "cookie" is also used to refer to these technologies. Technologies functionally similar to cookies include:

- The built-in storage mechanism of HTML5, in which user and device information can be stored and read during each session (session storage) or over a longer

period (local storage). The HTML storage mechanism can store character strings similar to actual cookie data. The HTML5 storage mechanism can also be utilised to implement functions similar to cookies. HTML storage procedures are typically implemented using JavaScript.

- Tracking technologies based on online requests allow the use of website or email content to be monitored. These technologies include tracking pixels, web beacons and various tags. The technology is typically implemented as an embedded invisible image on a site or in an email message. When the user opens a message or a site containing such technology, the device sends a request to download the content. As part of this request, data such as device IP address, date and time, and the requesting browser or email application type is transmitted to the server of the message sender or service provider. However, other types of data may also be requested.
- The user's device can also be identified by the use of fingerprinting technologies. In this situation, data available from the device through various methods is combined so that the device can be identified. User devices can also be identified via various device identification tags, such as advertising IDs (the "Advertising ID" of Android devices or the "IDFA Identifier for advertisers" in Apple devices).

Websites and online services may also collect a variety of user data, such as IP addresses and device and advertising IDs, as well as information on which websites have been visited at which hours, which contents have been accessed and which products have been purchased. Alone, these details might not constitute personal data pertinent to the user, but the more extensive the collection and combination of this information becomes, the more likely it is that the data collected does constitute personal data. This is likely especially when the information is collected for the purposes of profiling, targeting or influencing. In some cases, the information collected about the users of websites or online services is so detailed that it constitutes sensitive personal data, especially when health information is concerned. Processing personal data must always comply with the EU's General Data Protection Regulation (GDPR). Depending on the technology, other provisions may also need to be followed. In addition to the Act on Electronic Communication Services, the use of cookies must also comply with the GDPR as applicable.

3 Prerequisites for using cookies

3.1 General starting points

The general requirement for storing and using cookies or other forms of data on the user's actions in online services is that the **user has given their consent**. However, requesting consent is not required for setting up *essential* cookies or other similar technologies, i.e. when:

- the sole purpose of storing and using the data is to enable the transmission of messages in communications networks or
- the storage and use of the data is necessary for the service provider to provide a service that the subscriber or user has specifically requested.

Even in this situation, storage and use of data is only allowed to the extent necessary to provide the service, and even then, protection of privacy may not be restricted any more than is necessary.

It should be noted that legitimate interest does not authorise the storing or use of cookies or other data concerning the user's interaction with online services. Rather, this must be based on the grounds listed in section 205 of the Act on Electronic

Communications Services (917/2014). The section in question and the underlying Article 5(3) of the Directive on privacy and electronic communications do not recognise legitimate interest as a basis for storing or using cookies or other data on the user's interaction with online services on user devices. This means that legitimate interest is not a valid ground for using cookies or similar tracking technologies.

3.2 Exceptions to requesting consent

The law does not classify different types of cookies based on their technical or other characteristics. Whether a cookie is essential in the sense used in the law cannot be determined simply on the basis of its type or name because a single cookie can perform various functionalities and can be used for various purposes. The purpose of use for the data that is collected and processed using cookies is therefore critical when assessing which cookies could be considered essential.

The use of cookies or similar technologies that are considered essential does not require user consent. As noted above, *only* cookies and other data intended solely for transmitting messages in communications networks, or cookies and other data that are necessary for the service provider to provide a service that the subscriber or user has specifically requested are considered essential.

To be covered by the exception concerning the transmission of messages, the sole purpose of a cookie must therefore be to enable the transmission of messages. If cookies are only used to facilitate, speed up or in any way manage the aforementioned basic requirements, they are not covered by the exception. For the exception to apply, the cookie must therefore directly enable or implement one or more of the following:

- implement the transmission of a message through a network, by (for example) identifying the transmission points required for routing the message
- ensure the transmission of message content to the destination in an appropriate order
- identify errors or data losses occurring during the transmission of the message.

For example, load balancing is a technology that allows multiple background servers to process incoming requests to a site. The purpose of load balancing is to improve reliability and availability, and it can be implemented through various methods. If load balancing requires a cookie to be stored on the user’s device to ensure the user’s connections are always processed on a specific server for the requested service to function properly, the cookie in question can be considered necessary to transmit the message and thus essential. Third-party cookies are generally not required to transmit messages.

Essential cookies may also be required for the technical implementation of a user’s specific request on a website. The next section provides examples of different cookie types and guidance for the assessment on whether consent needs to be requested for their use.

3.3 Examples of different cookie types and guidelines for assessing the need for consent

- Authentication-related cookies

Cookies related to authentication are used to authenticate users logging into sites or applications. Session-specific authentication cookies are used to enable users to access the secure parts of a site and maintain the user's login while they are navigating and using the site. In addition to session-specific cookies, sites and applications may use more persistent login cookies that enable them to remember the user's login credentials or to maintain the user's login across several sessions. Session-specific cookies are more likely to be considered essential cookies as logging in to a service is an action that the user clearly chooses to take, and since no information is stored in the long term. Setting a permanent login cookie may, in some cases, improve usability and constitute a service explicitly requested by the user, especially if the user is provided with a choice for the long-term storage of login credentials. However, permanent login cookies cannot be automatically considered essential cookies if the user does not understand or cannot assume that long-term login will be maintained. Remembering login credentials and setting permanent login cookies without user consent might also in some cases constitute a risk to information security, especially in case of shared devices with more than one user. This needs to be taken into account when considering the term of validity for authentication cookies. In addition, if authentication cookies are used for secondary purposes, such as user tracking or targeted advertising, no exception can be made and user consent must be obtained.

- Cookies related to the user's preferences

  This cookie type can be used to remember aspects such as language choices and appearance and accessibility settings, such as the font, text size and how many search results to display per page of websites and applications. Preference cookies may also be used to store information related to user actions or preferences that can be used to offer customised actions or content. Preference or personalisation cookies may also be set per session. In this case the choices made will only be remembered for the duration of the session. However, they may also be set for a longer term, which makes it possible to collect and remember information across sessions. An example of a long-term preference cookie is remembering the user's home address for a route search when using a route planner website or application so the user does not have to enter the information again every time. Enabling and remembering language and appearance choices within each session serves the usability of the site, which can be considered an essential feature for offering the service, while offering recommendations based on page history or site navigation does not necessarily constitute a service explicitly requested by the user without asking consent. When assessing whether preference or personalisation cookies could be considered essential, user expectations concerning the service in question need to be taken into account. If the website or service can primarily be understood to offer a service that is personalised, personalisation cookies could be considered essential to be able to provide the service explicitly requested by the user.

- Cookies related to the user's input

  These cookies may be required for remembering the content of a user's shopping cart in an online store, or for remembering the content of the online service form they have completed. They are often related to a user action. In this case, enabling the user action to be carried out can be considered a service explicitly requested by the user. Without such actions, making orders or carrying out official business online would not be possible; therefore, cookies that enable functions such as these can be considered essential.

- Cookies related to targeted advertisement and marketing

  The use of cookies to create a profile of the user or the user's objects of interest, or to collect history data of user actions on websites or across several websites that can be used to display targeted advertising for the user cannot be considered essential for the production of a service explicitly requested by the user. Their use is therefore subject to consent.

- Cookies related to information security

  Cookies related to information security are used to ensure safe transmission of data between the user and the service. These cookies may, for example, be used to identify possible misuses or attempted misuses of the service by monitoring the number of successive failed login attempts. Some sites also use various mechanisms to identify whether the user of the service is a human. Examples of these include image recognition CAPTCHAs. In case of a method like this requiring a cookie to be stored on the user's device, the cookie can be considered essential for the safe use of the service; hence no consent needs to be requested.

- Cookies related to social media platforms

  Plug-ins, tools and extensions connected to social media platforms can be used on websites. If the use of such features on a website leads to cookies being stored on the user’s device, despite the fact that the user is not using the functionalities in question and/or is not a member of or signed into the said social media platform, consent must be requested for the cookies.

- Cookies related to accessibility

  When the sole purpose of cookies is to improve the accessibility of a site by (for example) enabling the use of audio description or voice subtitling, they can be considered essential. The use of these features is typically related to the service the user has explicitly requested.

- Analytics cookies

  These cookies are used to collect data on how visitors to a site use the service by recording unique traffic sources (IP addresses), counting page views and measuring how site or application content is used using various methods. The information that is collected can be used for purposes such as research or product development. Collecting analytics information is useful for service providers as it enables them to collect very detailed information on how the websites or services that they offer are used. From the user's perspective, however, analytics cookies cannot unambiguously be considered essential for the production of a service explicitly requested by the user, as the user is not likely to use the service for the purpose of his or her actions being tracked, and most services can be offered without using such analytics. Moreover, the user cannot be assumed to be aware of the collection of statistical information on their actions if no consent is requested. If the analytics cookies of a service are to be considered absolutely essential for the provision of the service, the service provider must present clear grounds for the procedure and ensure the protection of user privacy by, for example, making sure that no data collected through analytics are shared with third parties and no individual users can be identified based on the data. This is

important especially if the service also uses other types of cookies that could be used to link the user to the data collected through analytics. Should the service provider be unable to ensure the above to a sufficient extent or to justify the use of the analytics as being essential for the provision of the service, consent for the analytics needs to be requested.

Working Party 29, the predecessor of the European Data Protection Board, has considered that from the perspective of the user, analytics cookies cannot automatically be considered essential for the provision of a service requested by the user.[1] Moreover, the European Data Protection Board has stated that "in most cases, collection of organisational metrics relating to a service or details of user engagement cannot be regarded as necessary for the provision of the service as the service could be delivered in the absence of processing such personal data."[2] When it comes to analytics, the European Data Protection Board also considers that instead of the performance of a contract it would generally be recommendable to apply an alternative lawful basis for data processing, such as consent.[3]

- Specific data acquired from a terminal device via active scanning

  When a user opens a site on the internet, a request is sent from the terminal device to the service provider's server to load the content of the page. The server where the request is sent receives certain information from the device, such as its IP address. In this case, the device can be requested to send more data about itself. If the purpose of collecting and using such data is to create a profile of the device and its user, consent to use such technology must first be requested.

- Cookies that enable real-time communication

  Sites can use chat functionalities to enable real-time communication between the user and service provider. Using the chat functionality may require cookies to be set up on the user's device. If the main purpose of the site is not explicitly offering a chat functionality, this constitutes a plug-in or additional service, and the cookies related to their function may not be stored on the user's device before the user has specifically requested the service, i.e. opened the chat window. When cookies are set only after opening a chat window, and the functionality of the chat service requires the use of cookies, the cookies can be considered essential for the provision of the requested service, and the request of consent is not required.[4]

- Cookies related to cross-media content

  These days, websites are often designed so that some of the site content may be located outside the service provider's own service. Viewing or using such embedded content may require cookies belonging to a third party that hosts the content to be stored on the user's device. In this situation, user information is transferred to a party other than the service provider whose site the user is visiting. Cookies related to a third party's content cannot be considered essential cookies, and consent must be requested before their use.

[1]ARTICLE 29 Data Protection Working Party Opinion 04/2012 on Cookie Consent Exemption, page 10
[2]European Data Protection Board's Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, page 15
[3]European Data Protection Board's Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, page 15
[4] Traficom has interpreted the use of cookies that enable real-time communication in the same manner also in its earlier decision, Traficom/682/09.09/2019.

- Cookies related to presenting content

  Websites generally involve the provision of various forms of content. If presenting such content technically requires a cookie, it may be considered essential. If the cookies are used for anything other than this technical function, such as monitoring the content the user has viewed, they may not be considered essential.

- Device location data

  The approximate location of a device can be determined on the basis of its public IP address from which it is transmitting. However, device location can be determined with a precision of a few metres through modern positioning technologies, which often utilise GPS geolocation. If location data (as specified in the Act on Electronic Communication Services) is stored and/or read in some way through the use of cookies, the user's consent must be requested beforehand. More information about the processing of location data can be found in chapter 6 of these guidelines.

A more detailed legal perspective on the use of cookies and other data on user actions in online services is given in chapter 6 of these guidelines.

4 Consent

In principle, the storing of cookies and comparable data on user devices and the use of this data requires the cancellable consent of the user, as well as understandable and comprehensive information concerning the purpose of the storage and use of data (see chapter 5 concerning informing). Only essential cookies (section 3.2) do not require the user's consent. This chapter also explains in more detail how consent must be given and how users must be able to withdraw their consent.

4.1 Giving consent

Service providers must ensure that user consent is requested and the information related to cookies is presented appropriately and at the right time when the user first accesses the service or the website. As user consent needs to be requested for non-essential cookies, it must be ensured that no non-essential cookies are set on the user's device before the user has made the relevant choices concerning the use of cookies.

To be valid, consent must fulfil the conditions laid down in the **General Data Protection Regulation (GDPR)**[5]. According to the GDPR, consent refers to any freely given, specific, informed and unambiguous indication of their wishes by which the data subject, either by a statement or a clear affirmative action, signifies agreement to the processing of personal data relating to them. Consent must be an active expression indicating the data subject's wish. Silence, pre-ticked boxes or inactivity should therefore not constitute as consent.

[5] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and the free movement of such data, and repealing Directive 95/46/EC (GDPR)

In addition, refusing to give consent must be as uncomplicated as granting the consent. In the case of cookies this means that granting consent for non-essential cookies must not be any less complicated than refusing consent. Example: If an "Accept or allow all" selection is offered for granting consent for all non-essential cookies on the top level of the consent mechanism, a similar option to continue using the service only with essential cookies or to refuse consent for non-essential cookies should also be offered. In this case, granting and refusing to grant consent are equally easy or uncomplicated. In addition to these choices, the user should be provided with an option to make more detailed choices on consenting to the use of different types of cookies.

In the mechanism used for requesting user consent, it should also be ensured that the option to control all non-essential cookies used by the service, even third-party cookies, is offered. Further information about up-to-date privacy policies of third parties can also be provided by incorporating links to third-party privacy statements to the service provider's cookie mechanism or website. When using content or tools that set third-party cookies it is important to be aware of whether the information is processed in the role of jointly responsible data controllers or as a data controller and a data processor, as this has bearing on how responsibility is distributed.

However, the mechanism used to request consent should not unduly disrupt or prevent the user from accessing the site or service. If the user continues to access the service without making the choices concerning cookies, the site must only use essential cookies by default. It is therefore inappropriate to use the acceptance of non-essential cookies as a precondition for entering the site, because the consent cannot be considered voluntary in this case.[6]

The user's consent may be requested using a banner or a pop-up window that opens when the user visits the site. Pop-up windows may be automatically blocked through the settings of modern internet browsers, or the user may specifically block them. In this case, a banner is a more reliable option. Browser settings cannot be considered sufficient indications of consent, because the user may not have configured or may not have been able to configure the settings to suit their preferences. Moreover, configuring browser settings cannot be considered a sufficiently individualising and active expression of will for the purpose of accepting cookies that can be used to collect data for a variety of purposes.

Nor can the general terms and conditions of the service, accepting them or continuing to use the service be considered valid indications of consent. Obtaining consent must be a separate action containing a freely given, informed, specific and unambiguous expression of will. In the case of applications, obtaining consent before installing the application on a device can be technically challenging. This is why the purpose of storing and processing of information as well as the device permissions required by the application should be described as transparently as possible in the application's description in the application store. This is also why an option for controlling consent and making choices concerning non-essential cookies should be provided for the user after the installation of the application at the latest.

Cookie banners may not include pre-ticked boxes or slide switches in the "ON" position for non-essential cookies. Therefore, non-essential cookies may not be turned

[6] On the interpretation of consent, see the guidelines 05/2020 of 4 May 2020 on consent in accordance with Regulation 2016/679.

on by the service or the website by default, and the user must explicitly agree to their use by clicking on them (opt-in).[7]

4.2 Withdrawal of consent

According to the GDPR, users must be able to withdraw their consent at any time. Withdrawing consent or changing settings set earlier must be as simple for the user as possible. If consent is obtained electronically through a single mouse click, screen swipe or button press, users must be able to refuse or withdraw consent just as easily. Users must also be able to withdraw consent without detriment. This means that the service provider must ensure that withdrawal of consent can be done free of charge and without artificially reducing the quality of the service. However, withdrawal of consent for personalisation cookies, for example, may result in some degree of degradation of service quality and user experience.

Providing instructions on withdrawing consent or changing cookie choices when requesting consent should be considered good practice. The method that is provided must be in line with how consent was originally requested. For example, if consent was requested using a settings banner, the user should be able to easily access the banner again and change the cookie settings at any time by clicking on an icon visible on the page. The presentation of the consent mechanism can also be implemented through a link, but in this case, the location of the link should be communicated to the user clearly, and the link should be easily available on the site.

The service provider must ensure that withdrawing consent and changing settings has an actual effect. With regard to cookies, this means that implementing the procedure deletes or overwrites the data previously stored on the device.

4.3 Demonstration of consent

When requesting consent for the storage and use of data, it is appropriate to save the user's choices to ensure that consent does not need to be constantly requested while the user navigates the site. Saving the choices made through the consent mechanism may require the page to store a cookie that remembers the user's choices on the user's device.

The service provider must later be able to prove that they have requested consent to store and use cookies and comparable data. To prove consent, at least the following must be stored:

- date and time when consent was requested and obtained
- how consent was requested
- what information was provided to request consent, and
- the credentials that identify by whom and or from which device consent was given.

However, no more data may be stored than is necessary to prove the obtaining of consent. With regard to proving that consent has been requested and granted, it is recommendable to consider what is the reasonable duration that this information should be stored for. The user might use the site just once, occasionally or every day; therefore the reasonable amount of time can be determined through an esti-

[7]See also the judgment of the Court of Justice of the European Union of 1 October 2019 in Case C-673/17.

mation of average use cases, for example. The storage time could also be determined in relation to the validity of other cookies used. Moreover, consent must be requested again in case there are changes in the cookies used by the service.

With regard to the storage of personal data, it must be remembered that the data controller must plan and be able to justify the storage times of personal data. The storage time of personal data must also be documented. The GDPR does not define specific storage times for personal information. The data controller must estimate the appropriate storage period of personal data and whether it is necessary with regard to the purpose. Personal data may only be stored for the duration necessary for the purpose of processing the personal data. The data must be deleted when there no longer is a basis for processing the data.

5 Informing the users

Users must be informed of the use and storage of cookies and other data that requires user consent comprehensively and understandably. This information must be provided when the user makes the decisions on granting, rejecting or withdrawing consent. It is also recommended to inform users of cookies and similar technologies and the data collected through them even when no consent is legally required.

Banners or other mechanisms for requesting consent should, at minimum, specify the following:

- whether cookies and similar technologies are used; if yes, also their type
  - to give an example, the following classification may be used: essential, functional, personalisation, advertising, social media, analytics, others;
- the purpose of each cookie, i.e., what data is collected with the cookie and for what purpose
- the validity period of each cookie
- information on whether data collected using cookies is shared with third parties, who the third parties are, and what data is transmitted.

In addition to this, the banner may include more specific information or a link to more specific information concerning the cookies or privacy policy of the service.

It should also be noted that Article 13 of the GDPR concerning informing is also applied with regard to personal data.

6 Legislation and legal practice

6.1 Legislation

In Finnish legislation, provisions concerning the storage and use of cookies and other data on user actions in online services as well as the conditions that govern their use are set out in **section 205 of the Act on Electronic Communications Services (917/2014):**

> *The service provider may save cookies or other data concerning the use of the service in the user's terminal device, and use such data, if the user has given his or her consent thereto and the service provider gives the user comprehensible and complete information on the purposes of saving or using such data.*

Provisions of subsection 1 above do not apply to any storage or use of data which is intended solely for the purpose of enabling the transmission of messages in communications networks or which is necessary for the service provider to provide a service that the subscriber or user has specifically requested.

The storage and use of data referred to above in this section is allowed only to the extent required for the service, and it may not limit the protection of privacy any more than is necessary.

The national legislation was introduced on the basis of Article 3(5) of the **Directive on privacy and electronic communications**[8], according to which 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.

The Directive on privacy and electronic communication was amended to its current form in 2009 as part of the **"Cookie Law"**[9], which set the subscriber's or user's consent as a requirement for the storage of data or the use of data stored on the subscriber's or user's terminal device.

Storing of data on user actions in online services on user devices and the use of this data was nationally regulated by **section 7 of the Act on the Protection of Privacy in Electronic Communications** (the Act has since then been repealed). The section in question was amended in 2011 with the **national implementation of the Cookie Law**[10] so that even in national legislation, the storage and use of data on user actions in online services required the user's consent. The Act on the Protection of Privacy in Electronic Communications was repealed in 2014, and was replaced with the Act on Electronic Communications Services (the original name of the Act was the Information Society Code).

The consent required for the storage and use of cookies and other data on user actions in online services was interpreted according to the previously repealed **Data Protection Directive**[11], because according to Article 2(1) of the Directive on privacy and electronic communications, the Directive in question applies definitions included in Directive 95/46/EC.

[8] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 on the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications).
[9] Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009, amending Directive 2002/22/EC on universal service and users' rights related to electronic communications networks and services, Directive 2002/58/EC on the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws.
[10] Government Proposal HE 238/2010 on acts for amending the Communications Market Act, the Act on Radio Frequencies and Telecommunications Equipment, the Act on the Protection of Privacy in Electronic Communications and the Act on Certain Proceedings before the Market Court.
[11] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.

The methods for giving consent were also discussed in Recital 66 of the introductory part of the Cookie Law, according to which a user may give their consent to the storage of data on the user's terminal device or the use of data stored on the user's terminal device by using the appropriate settings of a browser or other application. The existence of this possibility was also explicitly stated in the national implementation of the Cookie Law, during which it was stated that "providing information and rejecting storage should be implemented in the most user-friendly manner possible. The user could thus give consent as described in the section through the settings of a browser or other application, for example."

Based on the above, the national interpretation by authorities regarding cookie consent has enabled the storage and use of cookies and other data on user actions in online services based on the user's browser settings.

The General Data Protection Regulation (GDPR) took effect on 25 May 2018 and changed the interpretation of consent given to the storage and use of cookies and data on user actions in online services. This is because according to According to Article 94(2) of the GDPR, references to the repealed Data Protection Directive are considered as references to the GDPR.

The GDPR set more detailed requirements for consent in comparison with the previous Data Protection Directive. According to Article 4(11) of the GDPR, consent "*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*".

In addition, Article 7 of the GDPR defines the requirements of consent in more detail. According to the article in question:

> *1. Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to the processing of his or her personal data.*
>
> *2. If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding.*
>
> *3. The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent.*
>
> *4. When assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is unnecessary for the performance of that contract.*

The concept of consent in accordance with section 205 of the Act on Electronic Communications Services and the requirements for giving it are therefore based on the provisions of the GDPR. Traficom is not the competent authority for interpreting consent as defined by the GDPR, but Traficom is authorised to interpret consent in accordance with section 205 of the Act on Electronic Communications Services.

When processing data collected on the basis of section 205 of the Act on Electronic Communications Services, it should also be noted that when the collected data constitutes personal data, the data must be processed in compliance with Article 13 of the GDPR concerning information to be provided to data subjects.

The EU is preparing a new regulation on privacy and electronic communications that will replace the Directive on privacy and electronic communications. At the same time, all legislation conflicting with the regulation must be repealed. According to the current **proposal**, the end user could give their consent for the storing of cookies, for example, by "whitelisting" one or more service providers in their browser settings. The legislative procedure within the EU is still in progress, and the final content and date of completion of the regulation remain uncertain.

On March 2019, the European Data Protection Board provided **instructions**[12] for implementing the Directive on Privacy and Electronic Communications (2002/58/EC) and the GDPR in a situation with linkages to both legal instruments. The instructions also contain examples related to cookies.

On the use of legitimate interest

It should be separately noted that the legitimate interest of a data controller as described in point (f) of Article 6(1) of the GDPR does not give a right to store cookies on the user's terminal device. Neither section 205 of the Act on Electronic Communications Services nor the underlying Article 5(3) of the Directive on Privacy and Electronic Communications recognises legitimate interest as valid grounds for the storing of cookies or other data describing the use of services on the user's terminal device and the use of such data. This means that legitimate interest is not considered a lawful ground for the use of cookies and other tracking technologies.

On the processing of location data

When processing cookies or other data on user actions in online services, the processing of the location data of the user's device is often brought into question. Provisions on the processing of location data are given in sections 160 to 162 of Chapter 20 of the Act on Electronic Communications Services. The competent authority for supervising this is the Data Protection Ombudsman.

Pursuant to section 160, subsection 1 of the Act, location data that can be associated with a natural person may be processed for the purpose of offering and using added value services, provided the subscriber or user to whom the data pertain has given consent or unless such consent is unambiguously implied from the context. Therefore, as a rule, the processing of location data concerning a user requires the user's consent.

6.2 Legal practice

Court of Justice on the European Union

On 1 October 2019, the Court of Justice of the European Union delivered their decision on cookies and the interpretation of consent required for their use in **Case C-673/17** (Planet49). In the judgement, the Court stated that consent given for storing cookies on the user's terminal device is not valid if consent is given by way of a pre-ticked checkbox on the website. According to the judgment, the service provider must also inform the user of the duration of the operation of cookies and whether or

[12] Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities. Adopted on 12 March 2019.

not third parties may have access to the cookies. Likewise, the Court ruled that whether the collected data can be interpreted as personal data or not has no bearing on requesting consent. Whether the data is technically anonymised is therefore irrelevant with regard to the storage and use of cookies or other data describing the use of services.

Helsinki Administrative Court

On 8 April 2021, The Helsinki Administrative Court delivered **two decisions** (H1515/2021 and H1516/2021 / Reg. no. 20801/2020 and 20848/2020) on the prerequisites for consent for the storing of non-essential cookies. The decisions ruled that because the default internet browser settings or those edited by the user generally allowed the use of various cookies, they could not be considered specific and informed indications of consent as referred to in Article 4(11) of the GDPR. In other words, the decisions ruled that browser settings do not constitute valid user consent on the storing of non-essential cookies on users' terminal devices.