Cookies and other data stored on users' terminal devices and the use of such data – Guidance 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 describing the use of services on the user's terminal equipment, 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.

The guidance is intended for everyone using cookies or similar technologies when implementing and providing websites or other electronic services.

The purpose of the instructions is not to obligate the use of specific technologies, but to instruct service providers to operate as required by law with regard to storing and using cookies and other data describing the use of services, requesting cookie consent and informing users about the use of cookies. Neither are these instructions intended to be exhaustive, and they will be updated accordingly as related technologies and legal practices develop.

This guidance has been compiled in collaboration with the Office of the Data Protection Ombudsman.

2 Scope of application

The instructions have been prepared for service providers who use cookies and similar techniques on their websites and electronic services, which allow storing of data to user's terminal equipment and reading of the data.

Cookies are small text files stored on terminal devices while using websites. Cookies contain data generated during the use of a site and between uses. Cookies and similar technologies enable the typical functionalities of modern websites, such as logging in and maintaining the login 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 visitors and their choices and inputs.

While these instructions primarily refer to cookies, it should be kept in mind that there are other technologies with functionalities similar to cookies. The same rules apply to these technologies, and these instructions should be followed where applicable. Examples of technologies similar to cookies are:

- A built-in storage mechanism in HTML5, in which data regarding users or their devices can be stored and read during a single session (session storage) or for a longer period (local storage). The HTML storage mechanism can store character sets similar to actual cookies. The HTML5 storage mechanism can be utilised to enable similar functionalities as cookies. HTML storage procedures are typically implemented using JavaScript.
- Previously, website content and interfaces were widely created using Adobe Flash. To use this type of content, the user's device must include software intended for reproducing it: Flash Player, a browser extension. When using Flash Player, data is stored on the user's device on local shared objects. The technology is therefore referred to as Flash cookies. Local shared objects can be used to store data similar to browser cookies, such as the user's unique identifier or data concerning the use of a site. Content using Flash-based and local shared object storage are currently used less frequently as other technologies are becoming more common, but the regulation also concerns them insofar as they are still in use.
- Request based technologies allow the use of the content of a website or email to be monitored. Such technologies include "tracking pixels", web beacons and various tags. The technology is typically implemented as an embedded image on a site or email so that it is invisible to the user. When a user opens a message or site containing such data, the device sends a request to download the content. As part of this request, data concerning the terminal device's IP address, the time of day, and the type of program used to read the requesting browser or email is transmitted to the server of the message sender or service provider. However, other types of data may also be requested.
- The user's terminal 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.

3 Prerequisites for using cookies

3.1 General starting points

The general prerequisite for storing and using cookies or other forms of data that describe the use of services is that the **user has given their consent**. However,

requesting consent is unnecessary to set up *essential* cookies or other corresponding technologies, i.e. when:

- the sole purpose of storing and accessing data is for carrying out or facilitating the transmission of a communication over an electronic communications network; or
- the storage and use of data is strictly 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, privacy protection may not be limited any more than is necessary.

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 the data collected and processed with cookies is therefore decisive to assess the essentiality of cookies.

It should be noted that the legitimate interest does not authorise the storing or use of cookies or other data that describes the use of 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 describing the use of services on the user's terminal device. This means that legitimate interest is not an appropriate legal basis for using cookies or corresponding tracking technologies.

3.2 Examples of cookies that require the user's consent

- Long-term cookies related to personalisation

  These or similar technologies are used to store data that enables the provision of customised functions and content and is also stored between sessions, i.e. the time between visits. An example is a cookie that remembers the user's home address for planning a route on map-based websites or applications.

- Authentication-related long-term cookies

  If the cookie is used to remember the user's authentication data between visits to the site and times when the application is used, consent to save the cookie should be requested.

- Development and analytics cookies

  Such cookies are used to collect data on how visitors to a site use the service by storing unique traffic sources (IP addresses), counting page views and measuring through various methods how website content is used. These cookies may also be related to research or product development. From a user's perspective, it is difficult to view such cookies as essential for providing a service that the user has specifically requested, even though the use of these cookies may be useful from the service provider's perspective.

- Cookies related to targeted advertisements and marketing

Consent is required for the use of cookies that allow creating a profile of the user and their interests, or which can collect data concerning the user's actions on sites for showing targeted advertisements or content.

- 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 also 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 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 social media platform, consent must be requested for the cookies.

- Cookies enabling 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 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.[1]

- Cookies related to cross-media content

  These days, websites are often created so that part of the available 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 hosting the content to be stored on the user's device. In this situation, data is shared with a party other than the service provider whose site the user is visiting. Cookies related to third-party content cannot in principle be considered essential cookies, and consent must be requested before their use.

- Exact location data of the device

  The approximate location of a device can be determined on the basis of its public IP address from which it is transmitting. However, the device's location within a few metres can be determined thanks to modern positioning methods, which often utilise the device's GPS data. If exact location data is stored and/or read in some way through the use of cookies, the user's consent must be requested

[1] 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.

first. More information about the processing of location data can be found in chapter 6 of these instructions.

3.3 Examples of cookies that do not require the user's consent

The use of cookies or similar technologies that are considered essential does not require requesting user consent. As stated above, *only* cookies and other data intended solely for carrying out transmission of a communication over electronic communications network, or which are strictly necessary for the service provider to provide a service that the subscriber or user has explicitly requested, are considered essential.

To be covered by the exemption concerning the transmission of message, 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 exemption. For the exemption to be applied, the cookie must therefore directly enable or implement one or more of the following:

- implement the transmission of a message through a network, by identifying the transmission points required for routing the message, for example
- ensure the transmission of the message's content to the destination in an appropriate order
- detect 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 following are examples of cookies considered essential to provide a requested service:

- Cookies related to the user's input

  These cookies may be required, for example, to remember the content of a user's shopping cart in an online store or the content of a form a user has completed online.

- Short-term cookies related to authentication

  Cookies related to authentication are used to authenticate a user logging into a site or service. Authentication cookies are typically session-specific and are used to enable users to access the secure parts of a site and maintain the user's login when they are navigating the site and using it. It should be noted that session-specific authentication cookies differ from persistent login cookies, which allow sites to remember the user's login data between visits to the site. The exemption therefore cannot in principle be applied to persistent login cookies. In addition, if the authentication cookies are used for a secondary purpose such as a targeted advertisements, the exemption may not be applied.

- Cookies related to information security

  Cookies related to information security are used to ensure the safe transmission of data between the user and the service. These cookies may be used to identify possible or attempted misuses of the service by monitoring the amount of successive login attempts, for example. Some sites also use various mechanisms to identify whether the user of the service is a human. Examples of these include image recognition CAPTCHAs. If the use of these methods requires a cookie to be stored on the user's device, it may be considered essential.

- 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. For example, the formerly widely used Flash technology-based content often required data to be stored on a device's local shared object directory. Such cookies were therefore considered essential to use such content. If the cookies are used for anything other than the aforementioned technical functionality, such as monitoring the content the user has viewed, they may not be considered essential.

- Cookies related to the user's preferences

  Examples of cookies related to preferences may include those that remember the user's choices regarding language, appearance and accessibility while visiting the site, such as the font or text size.

- Cookies related to accessibility

  When the sole purpose of cookies is to improve the accessibility of a site for example by 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 specifically requested.

- Cookies related to the site layout

  Websites can be implemented so that the presentation and layout of the site change according to the device used by the user visiting the site. For example, when viewing a site with a mobile device, a smaller version of the site is presented to better fit the smaller screen size than that of a computer. If the sole purpose of a cookie is to identify the device type for this kind of functionality, the cookie can be considered essential for the functionality of the service.

  The use of cookies and other data describing the use of services from the legal perspective is explained in more detail in chapter 6 of these instructions.

4 Consent

In principle, the storing of cookies and comparable data on user devices and the use of this data requires the withdrawable 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 3.3) do not require the user's consent. Among other things, this chapter explains in more

detail how consent should be given and how users should be able to withdraw their consent.

4.1 Giving consent

Service providers must ensure that the user's consent is requested, and that the information related to cookies is presented appropriately and at the correct time when the user opens the service or accesses the website. To be valid, consent must fulfil the conditions laid down in the **General Data Protection Regulation (GDPR)**[2]. 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 consent. In addition, refusing to give consent should be as easy as giving it.

With regard to the mechanism for requesting consent, it should also be ensured that it enables users to control at least all non-essential cookies used by the service, including third-party cookies. 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 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 consent cannot be considered voluntarily given in this case.[3]

The user's consent may be requested through the use of a banner or pop-up window that opens when the user visits the site, for example. Pop-up windows may be automatically blocked on the settings of modern internet browsers (or the user has personally blocked 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. 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.

With regard to non-essential cookies, the cookie banner may not include pre-ticked boxes or slide switches in the on position. Therefore, non-essential cookies may not be turned on in the service or site by default, and the user must separately agree to their use by clicking on them (opt-in).

The user may not be directed to make choices on the basis of colours used, nor may the action indicating rejection be less visible than the action indicating consent, by being placed on a different page of the consent mechanism or by being presented in a smaller font, for example. With regard to the visual presentation of the consent mechanism, the layout must be as neutral as possible.

[2] 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)

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

4.2 Withdrawal of consent

According to the GDPR, persons must be able to withdraw their consent at any time. Withdrawing consent or changing settings already set must be as simple for the user as possible. When 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. Among other things, this means the service provider must ensure that the withdrawal of consent can be done free of charge and without reducing the quality of the service.

Providing instructions on withdrawing consent or changing cookie choices already while requesting consent may be considered good practice. The provided method must be in line with how consent was originally requested. For example, if consent was requested with the use of a settings banner, the user should be able to easily view 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 requested by the consent mechanism may require the page to store on the user's device a cookie that remembers the user's choices.

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, the following must at least be stored:

- the moment when consent was requested and obtained;
- how consent was requested;
- what information was provided to request consent; and
- the necessary identification data with regard to who gave consent.

However, no more data may be stored than is necessary to prove the obtaining of consent. With regard to proving the obtaining of consent, it is a good idea to think about the reasonable duration for which data concerning the choices are kept. A single user's use of a site may be a one-off, random or daily occasion, and so the reasonable amount of time may be determined from an estimation of the average use cases, for example. The appropriate storage time should also be considered in relation to the validity of other cookies used.

With regard to the storage of personal data, it must be remembered that the data controller must design and be able to justify the storage times of personal data. The storage time of personal data must also be documented. Specific storage periods for personal data have not been defined in the GDPR. The data controller must estimate the storage period of personal data and the necessity with regard to the purpose of processing. Personal data may only be stored for the duration necessary for the

purposes of processing personal data. The data must be deleted when there is no longer a basis for their processing.

5 Informing users

Users must be informed comprehensively and understandably of the use or storage of cookies and other data that require user consent. This information must be provided when the user makes decisions on giving, rejecting or withdrawing consent. It is also recommended to inform users of cookies and other comparable technologies, as well as the data achieved through their use, even when they do not require consent according to the law.

Banners or other mechanisms for requesting consent should specify at least:

- the cookies and similar technologies used, as well as their type
  - for example, the following classifications may be used: essential, functional, personalisation, advertisement, social media-related, analytics and measuring, 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 is shared with third parties via the cookies, who these parties are, and what data is transmitted.

In addition to these, the banner may include more specific information or a link to specific information concerning the service's cookies or privacy policy, for example.

When cookies concern personal data, Article 13 of the GDPR concerning information to be provided is also applied.

6 Legislation and case law

6.1 Legislation

In Finnish legislation, provisions concerning the storage and use of cookies and other data describing the use of services and the conditions governing their use are laid down 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 5(3) of the **Directive on privacy and electronic communications**[4], 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 directive"**[5], 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.

The storage of data describing the use of services on the user's terminal device 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 directive**[6] so that even in national legislation, the storage and use of data describing the use of services required the user's consent. The Act on the Protection of Privacy in Electronic Communications was repealed in 2014, when it 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 describing the use of services was interpreted according to the previously repealed **Data Protection Directive**[7], 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.

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 directive during which it was stated that "providing information and rejecting storage should be implemented in the most user-friendly

[4] 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).
[5] 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 relating to electronic communications networks and services, Directive 2002/58/EC concerning 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.
[6] HE 238/2010 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.
[7] 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.

manner possible. The user could thus give consent as described in the section through the settings of a browser or other application, for example."

On the basis of the above, the national interpretation by authorities regarding cookie consent has enabled the storage and use of cookies and other data describing the use of services on the basis of the user's browser settings.

The General Data Protection Regulation (GDPR) became enforceable on 25 May 2018, and it also changed the interpretation of consent given to the storage and use of cookies and data describing the use of 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 point 11 of Article 4(1) 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 for the regulation**, the end user could give their consent for the storing of cookies, for example, by "whitelisting" one or several 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 **Opinion**[8] for applying the Directive on Privacy and Electronic Communications (2002/58/EY) 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 Article 6(1)(f) 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 an appropriate legal basis 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 does not constitute valid consent required for the use of cookies and other tracking technologies.

On the processing of location data

When processing cookies or other data describing the use of services, the processing of the exact location data of the user's terminal 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 Case law

Court of Justice of 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 decision, 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 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

[8] 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.

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 settings of an internet browser, whether they are the default or those edited by the user, that allow the use of various cookies could not be considered specific and informed indications of consent as referred to in Article 4(1) 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.