Cookies and other data stored on users' terminal devices and their use – Advice for website users

To be published on the National Cyber Security Centre's (NCSC-FI) website (not as a separate document, such as the instructions for service providers)

Have you ever wondered why you are asked to give your consent for the use of cookies or other data to be stored on your terminal device? Or why you have to choose what information a mobile application on your phone may use? Service providers present these questions to ensure that they have your consent to access your information. This is why it is important to think about what you are allowing.

This site includes advice to support your decisions. The purpose of the instructions is to help you understand what cookies stored on your device and other similar technologies used in various services are, and what they are used for. The instructions also contain tips on how to influence what data is stored on your devices and to help you assess whether service providers and their cookie policies are complying with requirements of the law.

What are cookies, and what are they used for?

Cookies are small text files that are stored on your terminal equipment – such as a computer, tablet or phone – when you browse websites. Cookies contain character sets that enable the performing of certain functions. They also contain information regarding your interactions with sites. The purpose of cookies is not to harm your terminal equipment, nor do they read data from the equipment's hard drive or spread viruses. Data can be stored in cookies while you use online services or visit websites and also in between the visits.

Cookies and similar technologies provide various functionalities common to websites today. Cookies are widely used on public and commercial websites, and they are a key component of the safe, efficient and user-friendly functionality of digital services.

Cookies and corresponding technologies can be categorised according to their lifetime, origin and purpose.

Read more:

Lifetime

- Session cookies are stored on your terminal device only while you use a website or service, and are deleted when you close the browser. For example, session cookies enable website logins and online shop shopping cart functions, and help sites remember information you have filled in on forms or other functionalities that require the site to remember information about your actions.
- Stored cookies are stored on devices longer. The duration lasts according to the specifications on the cookie, or until you remove the cookie. These cookies can be used to remember preferences regarding a site's visual appearance or language selection, or the account and/or password used to log in. Stored cookies can also be used to collect data on how you navigate around a website. This information can be used to show targeted content or ads, for example.

Origin

- First-party cookies are set directly by that website you are visiting or by the domain of the organisation that owns the site.
- Third-party cookies are set by a domain other than the owner of the site or service you are visiting.

Purpose

- Strictly necessary cookies enable core functionalities required for the sites to be used, such as logging in to secure parts of a site, remembering the content of your shopping cart on online stores, the filling of forms or the security of websites. Essential cookies are typically set by the first party and are session-specific. The law does not require the request of consent to use such cookies, but it is nonetheless recommended to inform people of their use.
- Functional cookies are used to increase and improve the functionality of sites, but they are not absolutely necessary for the use of the site.
- Preference and personalisation cookies allow websites to remember, for example, your choices regarding language and font size or your login details between visits. Such cookies also allow data to be collected to target website content.
- Analytics and performance cookies collect data regarding how sites are used by calculating unique traffic sources and page views, or by measuring the loading time of pages or monitoring how content has been viewed, for example.
- Social media cookies typically allow content from various social media platforms to be presented, enable liking and sharing functionality, or the use of social media accounts to log in and make comments.
- Marketing cookies are used, for example, to collect data on your interests based on your online behaviour and show you targeted ads that match your interests.

What is consent, and when must it be requested?

Website and mobile application service providers, who want to store cookies on your terminal equipment and read data from them, must give you clear and comprehensible information on the cookies or similar technologies that they are

using and the type, purpose and operating time of the cookies. They must also request your consent for storing and using this data.

According to the law, consent is not required for necessary cookies if:

- the sole purpose of storing or using data is to carry out the transmission of a communication over an electronic communications network, or
- the storage and use of data are strictly necessary for the service provider to provide a service that the subscriber or service user has specifically requested.

Even with these cookies, service providers are recommended to provide similar descriptions as with non-essential cookies.

> Read more:
>
> Section 205 of the Act on Electronic Communications Services (917/2014) lays down provisions on cookies and other data stored on users' terminal devices. It should be noted that the data controller's *legitimate interest* as defined in the EU General Data Protection Regulation (GDPR) does not entitle the storing of cookies on the user's terminal device. This means that the legitimate interest is not an appropriate legal basis for using cookies or other tracking technologies.

In legislation, consent refers to any freely given, specific, informed and unambiguous indication of their wishes by which data subjects, either by a statement or a clear affirmative action, signify agreement to the processing of personal data relating to them.

The method of implementation of the mechanism for requesting consent is freely selectable by the service provider and is their responsibility. The following are signs of a proper way to obtain consent:

- The mechanism in use describes the use of cookies and similar technologies clearly and comprehensively.
- The mechanism specifies the various types of cookies or other technologies used on the site or service, including their purpose and validity.
- The user is informed whether some third parties have the right to process cookie data.

On websites, consent is typically requested with a banner or pop-up that informs the user of the use of cookies. We recommend that you read the banners on each site carefully and use them to select what data may be stored on your terminal devices and collected from them. Service providers may not gain valid consent for storing non-essential cookies by instructing you to change your browser settings or by stating that "by continuing the use of this site/service, you accept the use of cookies".

The installation of a mobile application typically requires your explicit action. The access rights that a mobile application requires from a device are typically specified in the app store on the information/additional information section of an application. It is advisable to read this section before downloading and installing an application. If the use of a mobile application requires cookies (e.g. if logging in to the app is implemented through a website), the user must be informed of the use of cookies, and if necessary, their consent must be requested before starting the use of the application and the storing of cookies.

The mechanism for requesting consent must include an easily accessible option for rejecting the use of non-essential cookies. For example, if a cookie banner is used as the mechanism for requesting consent, it may not include pre-ticked boxes indicating consent or slide switches in the on-position with regard to non-essential cookies. In other words, users must be able to freely choose whether to give consent to the use of non-essential cookies.

The withdrawal of consent or the changing of ready-made cookie choices must be as simple and easy for the user as possible. The manner of withdrawing consent must be in line with the method by which consent was originally obtained. For example, if consent was requested with a banner, the banner for editing cookie settings should easily become available again when the user clicks on an icon or link on the page.

The service provider is responsible for ensuring that the withdrawal of consent or editing of cookie settings on a website has an actual impact, i.e. that the procedure in question removes or overwrites the previously saved data.

How can I affect the use of cookies myself?

Cookie settings can be managed in addition to each website through the security settings of modern browsers or for example in the case of mobile applications through the phone's application settings.

Read more:

You can make changes to the use of cookies through your browser settings as follows:

- Browsers may be set to reject all third-party cookies by default.
- Some browsers allow site-specific settings with regard to accepting or rejecting cookies.
- Most browsers also allow the use of cookies to be prevented entirely. However, please note that if you reject the use of all cookies, some sites and functions you might want to use may stop working. This is because the implementation of certain functions is based on the essential cookies mentioned in these instructions.
- The use of a private (incognito) browsing mode. The use of this browsing mode prevents the search history, other site information and long-term cookies from being stored on the device. The private browsing mode of certain browsers prevents the storing of third-party cookies entirely. Cookies and site data are stored in the browser cache for the duration of browsing, and the data is deleted only after exiting incognito mode. It should be noted that incognito mode does not prevent all data from being visible to the service provider. The service provider may still see some data like the IP address from where the connection has been made.

Session-specific cookies are automatically deleted when the browser is closed. The simplest way to manage long-term cookies stored on the device is usually through the browser settings. For example, all long-term cookies may be deleted as a single action, or they may be configured to be deleted every time the browser is closed. On some browsers, it is possible to remove long-term cookies on a site-specific basis.

What to do if a service provider does not comply with the requirements?

If you encounter a website or application that has a suspicious cookie policy or is clearly infringing the law, you should first contact the service provider in question

and inform them about the matter. Service providers are generally pleased to receive feedback from their customers and will change their service based on this feedback. When contacting the service provider of a website or application, you may refer to the instructions published by Traficom: [Link to instructions for service providers]

If the service provider does not respond to your feedback, does not take action regarding the issue, or if the service provider's answer is inappropriate, you can file a complaint to Traficom. The complaint may be drafted in free form, for example, by using Traficom's service forms [link: https://www.traficom.fi/en/contact-form-other-matters-concerning-information-security]]. It should include at least the following information:

- The concerned website or application. For example, the entire address of the website and name of the service provider. Please note that Traficom acts as the competent authority for Finland, meaning that it supervises service providers that are established or operating in Finland.
- When the issue was discovered (the date at least).
- A brief description of why you consider the service provider's operations inappropriate.

Traficom may also request additional information concerning your terminal device or a copy of your communications with the service provider to perform a technical inspection on the matter.

Traficom may examine the complaint in a written procedure in accordance with the Administrative Procedure Act (434/2003). This means that after receiving your complaint, Traficom will request a statement concerning the matter from the service provider and issue a decision after hearing the parties concerned.

It will typically take several months for Traficom to process the administrative matter. It is possible to lodge an appeal against Traficom's decisions. Appeals are made to the Administrative Court.

If Traficom detects that the service provider has acted unlawfully, it may notify the service provider of the matter and obligate them to remedy the defect or neglect within a reasonable period. A conditional fine or a threat of terminating the operations or of having the act done at the defaulter's expense may be imposed as sanctions in support of the obligation. However, Traficom does not have the powers to order administrative sanctions such as the imposition of fines for unlawful procedure on the service provider for their cookie policy.