

Semel's Privacy Statement

Protecting your privacy is very important to Semel – we want to keep your personal data secure. On this page, you will find information on how we collect and store your personal data.

Semel Oy processes its customers' personal data in all of its operations lawfully, respecting the customers' rights and expectations. To us, confidentiality of communications is an essential part of privacy protection. When processing our customers' personal data and other customer information, we comply with the Finnish and Swedish legislation, including the General Data Protection Regulation (2016/679; the "GDPR") and other applicable national data protection laws in Sweden and Finland ("Data Protection Law") the regulations and instructions issued by the authorities, and the good data processing practice. The purpose of this statement is to describe the principles and practices that we at Semel follow to guarantee the protection of our customers' privacy, the confidentiality of communications, and other legitimate interests. In particular, this statement describes what information we collect about our customers and how we process and protect this information.

We will update this statement, if necessary, as our operations and services develop. We advise you to check for the latest version regularly.

What personal data we process

We process only the personal data that we need for providing agreed communications services and other services and for conducting our business. We collect personal data and other customer information when concluding contracts, when a person registers for one of our services, when our services are sold or used, or otherwise directly from the person themselves in different channels. We also collect data on the use of our electronic services and web pages, utilizing cookies and similar technologies (see "Cookies").

With personal data, we refer to all data that can be associated with a customer or a user of our services.

We process the following personal data, for example:

- 1) Basic details, such as name and contact information;
- 2) Demographic details, such as age, gender and native language;
- 3) Data related to the identification and registration of a customer or user, such as the information required in the management of mobile certificates.
- 4) Data related to the customer relationship, such as service, product and order details, invoicing, credit and payment details, marketing permissions and prohibitions, customer contacts and related recordings, such as calls to our customer service.
- 5) Data generated in connection with communications services and other services, such as value-added services, e.g. traffic data related to calls and email messages; information on the parties to communications, time of the connection, data transfer protocol, location data, and terminal-related data;
- 6) Other data on the service use, such as data collected by means of cookies and similar technologies in connection with Internet or mobile browsing.
- 7) Other data collected with the person's consent, such as what the person is interested in.

We can update and collect data from public registers, such as the Population Register Centre, Posti, the Robinson opt-out list of Suomen Asiakkuusmarkkinointiliitto (the Finnish Customer Marketing Association), and private registers in compliance with applicable regulations.

For what purpose we process personal data

The processing of personal data is always factually justified on the basis of our operations. We process personal data for legitimate purposes defined in the appropriate description of file. We may combine data collected in connection with different products and services in so far as the data have been collected for the same purpose. Personal data will only be available to authorized employees holding a position that requires them to process personal data to perform their work. Personal data is not processed for no longer than is necessary for the particular purpose. We fully comply with our statutory retention obligations and our internal retention time policies. We never process personal data in a manner that is inappropriate in view of the defined purpose.

The main purposes are:

Provision of services: We process personal data for the provision of agreed services, e.g. when providing communications services we collect data that are necessary for conveying a call from the caller to the recipient. The provision of services requires that we process personal data for identifying customers or users, processing and delivering orders, invoicing for the services, credit control, debt collection, customer service, and for fixing various faults and incidents or for processing complaints. We process personal data in customer communications, e.g. when sending notifications related to services, and in order to contact customers in issues related to our services.

Development and analysis: We process personal data for developing and managing our business and services and the related processes, such as sales and marketing, and for better understanding our customers' needs. We may process traffic data for the transmission of communications or for the technical development of a communications service, such as for optimizing the operations of communications networks. We may compile statistics to the extent necessary for developing products and services or for other analysis needs. We may group our customers based on invoicing, data volumes, the duration of the customer relationship or external classifications, e.g. draw up reports on how different user groups use communications services or how a person's residence and age affect their use of services.

Marketing and giving recommendations: We process and utilize both summed usage data and data associated with individuals for marketing purposes and for forming target groups for marketing. We may process personal data for personalizing and targeting services for instance by giving recommendations and by showing targeted contents in our services or customer channels. We may use personal data within the limits of the law for marketing both our own and our cooperation partners' products and services, such as for direct marketing and market research, and for customer satisfaction surveys.

Information security and misuse of services: We may process personal and traffic data in order to ensure the information security of all our services and communications networks. If necessary, we may also process personal data in order to detect or prevent various types of misuse of services, e.g. in such instances of misuse of communications services where a charged communications service has been used for free.

Compliance with statutory obligations: We process personal data in order to meet our statutory obligations, such as for accounting and authority purposes.

In all of the above cases, we process personal and traffic data only to the extent necessary for the purpose, always taking into account the protection of our customers' privacy.

On what criteria we process personal data

The processing of personal data is usually based on an agreement we have concluded or another relevant context, such as the use of our services. We may also process personal data based on other criteria, such as consent, assignment or the law. In so far as the processing of personal data is based on consent given by a person, the person has the right to freely cancel or otherwise govern their consent.

We process only the personal data that are necessary in view of the purpose defined in the applicable description of file. We may combine personal data in our different personal data files within the limits of the law.

We process the personal data or contact information of potential customers, when someone participates in a competition or customer event or contacts Semel. The data are stored and processed according to the description of file of our permanent direct marketing data file.

How we store personal data

We strive to ensure that the personal data and other customer information are up-to-date and accurate, taking into account the nature of the personal data processed. We do not keep outdated or unnecessary data.

We keep personal data only as long as necessary to fulfill the purposes defined. Even if the customer relationship has ended, we may still have a relevant connection with the person, for example because we must collect receivables,

because the person has filed a complaint, or because we must fulfill a direct marketing prohibition that the customer has given. Typically we keep the customer data for about three years after the end of the customer relationship. The law obliges us to keep certain data. The Accounting Act, for example, obliges us to keep all accounting records for 6 years. We must also retain certain communications-related data so that the authorities can utilize them when investigating the most serious offences. For this purpose, we must keep the traffic data related to calls and text messages in the mobile network, for example, for 12 months after the communications event.

Our customer's rights

- **Right to access and rectification:** You have the right to request access to the personal data relating to you. This includes e.g. the right to be informed whether or not personal data about you is being processed, what personal data is being processed, and the purpose of the processing. You also have the right to request that inaccurate or incomplete personal data be corrected. The customer can check this free of charge once a year. The request for checking the data must be submitted in a personally signed document or a similarly certified document.
- **Right to object:** You are entitled to object to certain processing of personal data, including for example processing of your personal data for marketing purposes or when we otherwise base our processing of you on a legitimate interest.
- **Right to erasure:** You may also request that your personal data be erased if e.g. the personal data is no longer necessary for the purposes for which it was collected, the processing is unlawful, or the personal data has to be erased to enable us to comply with a legal requirement.
- **Right to Data Portability:** If personal data about you that you yourself have provided is being processed automatically with your consent or in accordance with a contract between you and Semel, you may request that the data is provided in a structured, commonly used and machine-readable format and you may also request that the personal data is transmitted to another controller, if this is technically feasible.
- **Right to withdraw your consent:** In cases where the processing is based on your consent, you have the right to withdraw your consent to such processing at any time.
- **Opt-out from marketing:** We will also give you the opportunity to opt out of future marketing and prohibit us from using their data for direct advertising, distance selling and other direct marketing or for market research and opinion polls whenever we send you marketing material, you can also opt out at any time by contacting us. The customer can opt out of direct marketing by sending a written notification to Semel Oy, Customer Service, P.O. Box 1000, 00380 Helsinki. When opting out, the customer must provide the necessary identifying information.

Note that there may be situations where our confidentiality and other obligations under applicable legislation and the respective Bar Rules may prohibit us from disclosing or deleting your personal data or otherwise prevent you from exercising your rights, if the personal data relates to our client work.

If you have any complaints about how we process your personal data, or would like further information, please contact us at any time.

If you wish to file a complaint with a national data protection supervisor authority regarding our processing of your personal data, you may do so by contacting your local data protection authority ("local" meaning where you live or work, or where an alleged data breach has occurred). The relevant authority in Sweden is Datainspektionen (www.datainspektionen.se) and, in Finland, the Data Protection Ombudsman (www.tietosuoja.fi).

The customer's consent to the processing of traffic data for marketing purposes or the customer's electronic direct marketing permission for text message or email marketing may be requested in some of our services (e.g. a certain subscription type) under the terms of agreement. In addition, we request various marketing permissions separately from our customers. Even in these cases, the customer has the right to cancel their consent and forbid the processing

of their personal and traffic data for marketing purposes, but if the consent is related to a certain service, the service (e.g. a subscription type) may have to be changed for another one.

Even if the customer prohibited us from processing their personal data for marketing purposes, we can nevertheless continue to send them notifications about our services, e.g. information on amendments to the agreement or on faults or disturbances in the service.

Disclosure of personal data

The personal data of our customers and other customer information are confidential. We do not sell or disclose our customers' personal data to any third parties except in the cases specified below.

We may disclose our customers' personal data to other companies belonging to same group of companies as Semel within the limits of the law.

We may transfer our customers' personal data either in full or in part within the Group and to our external subcontractors in so far as they participate in the processing of personal data on our assignment. These third parties may not use the personal data for any other purpose than for fulfilling the purpose agreed with us. In this connection, personal data may be transferred between different countries. Although we, as a rule, do not transfer data outside the EU or EEA, the transfer may be necessary for the technical implementation of the processing of personal data.

Personal data may also be transferred to such countries outside the EEA where the legislation concerning the processing of personal data differs from that of Finland. Even in this case we will ensure that the protection of personal data is on an adequate level. We see to this, for example, by agreeing on issues related to the confidentiality and processing of personal data as required by law, using for instance standard contractual clauses approved by the European Commission, and by ensuring that personal data are always processed in compliance with the Finnish law and this privacy statement. In such cases, we inform our customers in an appropriate manner.

Customers' personal data can be disclosed to third parties for their own purposes, if the customer has given their consent to this.

We may also disclose the customer's personal data to a competent authority and, under a court order, to other parties, such as the holder of a copyright or their representative, if the applicable legislation so requires. Semel is under the obligation to disclose information on our customers to the extent required by law to, for example, the Finnish Communications Regulatory Authority (FICORA), the Data Protection Ombudsman, the Police, and the emergency centre authorities.

Under a confidentiality agreement, personal data may also be disclosed in connection with various mergers and acquisitions to the acquiring companies and their advisors for a predefined purpose.

Protection of personal data

We protect the personal data we process against outsiders and other unauthorized processors as efficiently as possible by means of various technical and organizational measures. We prevent any external parties from accessing our information systems and see to the security of data communications, the security of equipment spaces and similar facilities, the information security risks related to loss of data and other similar risks to the information security in an appropriate manner, taking into account the probability of the risk, the technical options, and the nature of the data to be protected.

Our information systems use advanced access right management, and the use of our information systems is monitored. Personal data and other customer information are only processed by those designated Semel employees or those persons working for Semel whose legitimate duties require the processing of personal data and other customer information. Our employees processing personal data and other customer information are under the obligation of secrecy regarding the data they process in their work. Our personnel are constantly trained on matters of privacy. When using subcontractors, we ensure, by means of agreements or in another appropriate manner, that even our subcontractors operate in accordance with this statement. We assess our processes related to the processing of personal data and the risks associated with them on a regular basis.

If we detect any information security breaches directed at our customers' personal data, we report them to the competent authority. We also notify the customer of any information security breach directed at their personal data that we are aware of, if the breach is likely to have a detrimental effect on the customer's privacy.

Security of services

We attend to the information security of our services and communications networks by applying practices that are appropriately proportioned to the gravity of the threats to be fought against on the one hand, and to the available technical level of development and costs on the other. We exercise great care in our measures to prevent information security breaches and disruptions, and aim in every way to prevent the confidentiality of communications or privacy protection from being unnecessarily jeopardized. When possible, we provide information on measures related to the information security of our services and on other issues related to information security in an appropriate manner, e.g. on our website or in customer bulletins. We may take necessary measures to prevent information security breaches and disruptions. For example, we may prevent the reception of email messages, remove viruses and malware from messages and carry out related technical measures to the extent permitted and required by law. When taking these measures, we always make sure that they are necessary for ensuring the availability of communications networks and services and for safeguarding our customers' communications. Our customers must also see to their own information security in an appropriate manner. We advise our customers to exercise care in the use of our services and in the storing of terminals and to monitor their use by means of various security or PIN codes. It is also important to ensure that sufficient virus and firewall services are used and that the services and operating systems are updated.

Processing of location data

We may process location data that indicate the geographical location of a subscription or terminal in various commercial value-added services, such as map, positioning and navigation services or in regionally targeted advertising services. The accuracy of location data in the mobile network is based on the number of base stations in the area concerned, and it can vary from hundreds of metres to several kilometres. The processing of location data is always based on prior consent of the person to be located. If we disclose location data to external service providers, we ensure in an appropriate manner that the persons to be located have given their consent.

To the extent permitted by applicable legislation, our customers have the right to receive the traffic data indicating the location of their subscription or terminal device.

Cookies

We may use cookies and similar technologies such as the browser's local data storage (hereafter "cookies") on Semel's website to collect information about a user's terminal device.

Cookies are files that the website, application or clicked advertisement sets in the user's web browser while the user is browsing that website. A cookie contains an anonymous individual identifier, which we can use to later identify various browsers or terminals on different web pages and in different services. Only the server that sent the cookie can later read or use the cookie. A user cannot be identified merely through cookies.

We use information collected by means of cookies typically for the following purposes:

Functional cookies and service provision: Cookies are very important for the operation of our website and electronic services, and they enable a smooth user experience.

Service development: By monitoring the use of cookies, we can improve the operation of our website and electronic services. We receive information, for example, on what the most popular sections of our website are, to which websites the users continue or from which websites they come from, and how long they stay on our website.

Network analysis: We use cookies to compile statistics on the number of visitors to our web pages and electronic services and to evaluate the efficiency of advertising. We may collect information, for example, from marketing emails and newsletters in order to find out whether the messages have been opened and whether actions have been taken on the basis of them, e.g. whether the user has clicked from the message to our website. We may also use cookies, for example, to find out whether our website and services are used on a computer or on a mobile device.

Targeting of marketing: By means of cookies, we may also collect information for providing advertisements or contents targeted at a certain browser by creating different target groups. Based on the collected information, the different target groups are shown advertisements or contents that are likely to be of interest to them on the websites or electronic services of Semel or its cooperation partners. We may, within the scope of the law, combine information received by means of cookies with information received on the user in other connections, such as information on the Semel services used.

Our customers can read about the cookies we use and their management here.

Cookies can be disabled in the browser settings. In some cases, this may slow down the browsing of our website or completely prevent access to a certain page. Disabling cookies will not prevent advertisements from being shown, but the advertisements or other content shown will not be adapted based on previously collected data.

The user can also clear cookies in the browser settings. In this case, the information previously collected by means of cookies is deleted, and the collection of information will start again from the beginning.

With our permission, third parties are allowed to set cookies on the user's terminal when the user visits our website, for example, in order to provide targeted advertising to the user or to compile statistics on the number of users on different web pages. Because the user's browser requests advertisements set by a third party from a server outside Semel, these third parties may view, edit or set their own cookies as if the user were on their own websites.

Our website may contain links and connections to the websites of third parties and social plugins of third parties, such as the Like button on Facebook or the Tweet button on Twitter. The buttons are shown on our website, but their content comes directly from the social network in question. When a user visits our service, the social plugin recognizes when the user is simultaneously logged in to the social network site in question and adapts the content of the page shown in the plugin as if the user were on the website of the social network. Adapted content is not shown unless the user is logged in to the website of the social network. More information on the privacy of social network services can be found on the website of the social network in question.

The third-party services, plugins or applications on Semel's website and in Semel's services are subject to the terms of use and other terms and conditions of the third party in question. With contractual arrangements, Semel makes sure that these third parties comply with applicable legislation and the self-regulatory guidelines of the industry.

Contact information

The customer can send any complaints about the targeting of advertising to:

Semel Oy
Customer Service
PL 1000
00380 Helsinki

Any inquiries related to this privacy statement can be sent to:

Semel Oy
Customer feedback / GDPR
PL 1000
00380 Helsinki

Contact information of the supervisory authorities

Data Protection Ombudsman
Ratapihantie 9, 6th floor, 00520 Helsinki
tietosuoja@om.fi
FICORA
Itämerenkatu 3 A, 00180 Helsinki
kirjaamo@viestintavirasto.fi

Laws applicable to the processing of personal data and traffic data

Personal Data Act (523/1999)

Information Society Code, Part VI, Confidentiality of Communications and Protection of Privacy (917/2014)

General Data Protection Regulation (2016/679; the "GDPR")